ANAGRAFICA AZIENDA

Azienda/Organizzazione	**FATEK s.r.l.**

SEDE LEGALE	Sede 1 Via Raffaello Morghen n°35, 10143 Torino - TO

Data revisione: 29/04/2019

DATI AZIENDA

Ragione Sociale	**FATEK s.r.l.**
Partita IVA	10786800010
Codice fiscale	10786800010
Sede legale	Via Raffaello Morghen n°35, 10143 Torino - TO
Contatti	- Tel: 011 0438596 - Email: info@fatek.it - PEC: fateksrl@legalmail.it
Sito web	www.fatek.it
Attività economica	Attività di fabbricazione
Codici ATECO	• 28.21.10 - Fabbricazione di forni, fornaci e bruciatori
Rappresentante legale	De Palo Michele
Codice fiscale	DPLMHL84P11F335R
Contatti	- Email: acquisti@fatek.it - PEC: fateksrl@legalmail.it

SEDI

Nome	**SEDE 1**
Tipo	- Legale
Indirizzo	Via Raffaello Morghen n°35, 10143 Torino - TO

Nome	**SEDE OPERATIVA**
Tipo	- Amministrativa - Operativa
Indirizzo	Via Lombardi n°8, 10028 Trofarello - TO

NOMINE

Soggetto	**KLW Consulting s.r.l.s.**, p.iva 11631640015
Contatti	- PEC: klwconsultingsrls@open.legalmail.it
Nomina	**Responsabile del trattamento esterno** Sede: Sede Operativa

Soggetto	**AMJ s.r.l.**, p.iva 10014130016
Contatti	- PEC: amjsrl@pec.it
Nomina	**Responsabile del trattamento esterno** Sede: Sede Operativa

Soggetto	**Danea Soft s.r.l.**, p.iva 03365450281
Contatti	- PEC: soft@pec.danea.it
Nomina	**Responsabile del trattamento esterno** Sede: Sede Operativa

Soggetto	**Linuxon di Marengo Piercarlo**, p.iva 09347810013
Contatti	- PEC: pmarengo@pec.linuxon.it
Nomina	**Responsabile del trattamento esterno** Sede: Sede Operativa

Soggetto	**Wea s.r.l.**, p.iva 07103660010
Contatti	- PEC: wea-group@pec.it
Nomina	**Responsabile del trattamento esterno** Sede: Sede Operativa

Soggetto	**De Palo Michele**, c.f. DPLMHL84P11F335R
Contatti	- Tel: 011 0438596 - Email: acquisti@fatek.it - PEC: fateksrl@legalmail.it
Nomina	**Titolare del trattamento** Sede: Sede Operativa

Soggetto	**Del Col Fabio**, c.f. DLCFBA72E06L219F
Contatti	- Email: direzione@fatek.it
Nomina	**Persona autorizzata** Sede: Sede Operativa

Soggetto	**Pozzo Roberta**, c.f. PZZRRT86C66L219C
Contatti	- Email: info@fatek.it
Nomina	**Persona autorizzata** Sede: Sede Operativa

PARTNERS

Nominativo	**KLW Consulting s.r.l.s.**
Tipo Partner	Partner/fornitore
Partita IVA	11631640015
Codice fiscale	11631640015
Indirizzo sede legale	Via Raffaello Morghen 35, 10143 Torino - TO
Contatti	- PEC: klwconsultingsrls@open.legalmail.it

Nominativo	**AMJ s.r.l.**
Tipo Partner	Partner/fornitore
Partita IVA	10014130016
Codice fiscale	10014130016
Indirizzo sede legale	Via Onorato Vigliani 51, 10135 Torino - TO
Contatti	- PEC: amjsrl@pec.it

Nominativo	**Danea Soft s.r.l.**
Tipo Partner	Partner/fornitore
Partita IVA	03365450281
Codice fiscale	03365450281
Indirizzo sede legale	Via A. Diaz 162, 35010 Vigonza - PD
Contatti	- PEC: soft@pec.danea.it

Nominativo	**Linuxon di Marengo Piercarlo**
Tipo Partner	Partner/fornitore
Partita IVA	09347810013
Codice fiscale	MRNPCR73B28L219P
Indirizzo sede legale	Via Villarbasse 2, 10090 Bruino - TO
Contatti	- PEC: pmarengo@pec.linuxon.it

Nominativo	**Wea s.r.l.**
Tipo Partner	Partner/fornitore
Partita IVA	07103660010
Codice fiscale	07103660010
Indirizzo sede legale	Via Michele Lessona 11, 10143 Torino - TO
Contatti	- PEC: wea-group@pec.it

Nominativo	**Gruppo IVA Credito Emiliano**
Tipo Partner	Partner/fornitore
Partita IVA	02823390352
Codice fiscale	02823390352
Indirizzo sede legale	Via Emilia A S. Pietro 4, 42121 Reggio Emilia - RE
Contatti	- PEC: credem@pec.gruppocredem.it

Nominativo	**Credito Valtellinese S.p.A.**
Tipo Partner	Partner/fornitore
Partita IVA	00043260140
Codice fiscale	00043260140
Indirizzo sede legale	Piazza Quadrivio 8, 23100 Sondrio - SO
Contatti	- PEC: creval@pec.creval.it

Nominativo	**BRT S.p.A.**
Tipo Partner	Partner/fornitore
Partita IVA	04507990150
Codice fiscale	04507990150
Indirizzo sede legale	Piazza Armando Diaz 7, 20123 Milano - MI
Contatti	- PEC: brt@pec.brt.it

Nominativo	**Corriere Gianotti Autotrasporti di Gianotti Giorgio & C. s.n.c.**
Tipo Partner	Partner/fornitore
Partita IVA	08644220017
Codice fiscale	08644220017
Indirizzo sede legale	Via Giacomo Matteotti 39, 10016 Montalto Dora - TO
Contatti	- PEC: gianotti.trasporti@pecimprese.it

ARCHIVI INFORMATICI

Nome	**PC 1 - Ufficio Operativo**
Tipo Struttura	Interna
Sede	Sede Operativa (Trofarello)
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	- Danea Soft - Pacchetto Office

Nome	**PC 2 - Ufficio Operativo**
Tipo Struttura	Interna
Sede	Sede Operativa (Trofarello)
Personale con diritti di accesso	Del Col Fabio, c.f. DLCFBA72E06L219F
Note	PC ad uso esclusivo del Sig. Del Col Fabio
Software utilizzati	- Danea Soft - Pacchetto Office

Nome	**PC 3 - Ufficio Operativo**
Tipo Struttura	Interna
Sede	Sede Operativa (Trofarello)
Personale con diritti di accesso	Pozzo Roberta, c.f. PZZRRT86C66L219C
Note	PC ad uso esclusivo della Sig.ra Pozzo Roberta
Software utilizzati	- Danea Soft - Pacchetto Office

Nome	**Server NAS**
Tipo Struttura	Interna
Sede	Sede Operativa (Trofarello)
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R Linuxon di Marengo Piercarlo, p.iva 09347810013
Note	Server in cui vengono backuppati giornalmente i dati presenti sui PC aziendali. E' dotato di due dischi fissi configurati con la tecnica RAID: ovvero tutto il contenuto che viene memorizzato nel primo disco viene automaticamente copiato anche nel secondo.

ORGANIGRAMMA GDPR

Azienda/Organizzazione **FATEK s.r.l.**

SEDE LEGALE	Sede 1 Via Raffaello Morghen n°35, 10143 Torino - TO

Data revisione: 29/04/2019

Di seguito, è riportato l'organigramma con le funzioni nominate per la gestione della protezione del trattamento dati personali:

SEDE OPERATIVA

Titolare del trattamento:	**De Palo Michele**	Data nomina: 26/03/2019

Responsabili esterni del trattamento:	**KLW Consulting s.r.l.s.**	Data nomina: 26/03/2019
	AMJ s.r.l.	Data nomina: 26/03/2019
	Danea Soft s.r.l.	Data nomina: 26/03/2019
	Linuxon di Marengo Piercarlo	Data nomina: 26/03/2019
	Wea s.r.l.	Data nomina: 26/03/2019

Persone autorizzate:	**Del Col Fabio**	Data nomina: 26/03/2019
	Pozzo Roberta	Data nomina: 26/03/2019

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Azienda/Organizzazione **FATEK s.r.l.**

REGISTRO	Registro Dipendenti

SEDE	Sede Operativa Via Lombardi n°8, 10028 Trofarello - TO

Data revisione: 29/04/2019

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato. Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	De Palo
	Nome	Michele
	E-mail	acquisti@fatek.it
	PEC	fateksrl@legalmail.it
	N° telefono	011 0438596

VALUTAZIONE DEL RISCHIO E MATRICE DI RISCHIO

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	**Improbabile**
2	**Poco probabile**
3	**Probabile**
4	**M. Probabile**
5	**Quasi certo**

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**
5	**Gravissime**

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(*1 ≤ *LR* ≤ 3*)*
Medio - basso	*(*4 ≤ *LR* ≤ 6*)*
Rilevante	*(*8 ≤ *LR* ≤ 12*)*
Alto	*(*15 ≤ *LR* ≤ 25*)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

TRATTAMENTO: Gestione del Rapporto di Lavoro
Scheda creata in data: 29/04/2019
Ultimo aggiornamento avvenuto in data: 29/04/2019

Struttura	• Sede operativa

Personale coinvolto	
Persone autorizzate	De Palo Michele (Rappresentante legale) • Conservazione • Consultazione • Raccolta
Partners - Responsabili esterni	AMJ s.r.l., p.iva 10014130016 (Consulente del Lavoro) • Conservazione • Consultazione • Elaborazione KLW Consulting s.r.l.s., p.iva 11631640015 (Commercialista) • Conservazione • Consultazione Wea s.r.l., p.iva 07103660010 (Azienda di Consulenza Sicurezza sul lavoro) • Conservazione • Consultazione • Elaborazione Linuxon di Marengo Piercarlo, p.iva 09347810013 (Società di manutenzione hardware e gestione Server) • Conservazione Credito Valtellinese S.p.A., p.iva 00043260140 (Istituto Bancario) • Conservazione Gruppo IVA Credito Emiliano, p.iva 02823390352 (Istituto Bancario) • Conservazione

Processo di trattamento	
Descrizione	Adempimento degli obblighi previsti dal Contratto di Lavoro o Collaborazione: ad esempio recupero dati per assunzione personale e per emissione buste paga, gestione dei turni lavoro, gestione dei giorni di malattia, ferie, contributi. Adempimento degli obblighi previsti dal D.Lgs 81/08: ad esempio recupero dati per effettuazione corsi di formazione obbligatori in materia di sicurezza sul lavoro, visite Medicina del Lavoro (ove richiesto), ecc.
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Legge Contratto
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Elaborazione buste paga Contratto di assunzione Bonifici per pagamento stipendio Adempimenti obblighi D.LGS. 81/08 Programmazione delle attività (pianificazione e monitoraggio del lavoro) Gestione del contenzioso Gestione dei turni lavoro, gestione dei giorni di malattia, ferie, contributi, ecc.
Tipo di dati personali	Nome e cognome, dati identificativi in generale inclusi residenza, e domicilio; codice fiscale; dati di natura finanziaria quali buste

	paga, certificati di reddito, IBAN; dati di natura sanitaria quali certificati medici, informazioni in genere circa la salute; informazioni relative a corsi di formazione e titoli di studio acquisiti; dati relativi alla contribuzione previdenziale e all'assicurazione dei lavoratori; dati relativi a fondi di categoria o assicurativi sottoscritti.
Categorie di interessati	Dipendenti o Collaboratori
Categorie di destinatari	Enti pubblici preposti alla Previdenza Sociale, all'Assicurazione dei Lavoratori e all'Accertamento Fiscale(esempio: INPS, INAIL, Agenzia delle Entrate etc.) e qualunque ente pubblico a cui l'azienda è tenuta a fornire i Dati dei propri dipendenti per obbligo di Legge. Enti di Formazione per l'erogazione di corsi di formazione e di aggiornamento professionale dei dipendenti oltreché per i corsi inerenti la sicurezza sul lavoro. Società e Professionisti deputati alla Medicina del Lavoro Società e Professionisti deputati alla gestione, alla manutenzione e all'assistenza da remoto dell'apparato informatico. Professionisti nel settore della Contabilità e della Gestione di Paghe e Contributi. Autorità Giudiziarie competenti.
Informativa	Si
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Mensile
Termine cancellazione dati	Sino al termine del rapporto di lavoro o collaborazione con lo studio. Nel caso vengano trattenuti anche Dati Personali soggetti ad obblighi di conservazione stabiliti dalla Legge Italiana od Europea entro e non oltre i limiti dettati dalla normativa di riferimento.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Pacchetto Office
Archiviazione	Armadio e/o Cassettiera chiusa a chiave.
Strutture informatiche di archiviazione	
PC 1 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale)
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	- Danea Soft - Pacchetto Office
Server NAS	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale) Linuxon di Marengo Piercarlo, p.iva 09347810013 (Società di manutenzione hardware e gestione Server)
Note	Server in cui vengono backuppati giornalmente i dati presenti sui PC aziendali. E' dotato di due dischi fissi configurati con la tecnica RAID: ovvero tutto il contenuto che viene memorizzato nel primo disco viene automaticamente copiato anche nel secondo.

Strutture informatiche di backup	
PC 1 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale)
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	- Danea Soft - Pacchetto Office

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Accessi limitati alle cartelle di propria competenza.
- Dispositivi antincendio
- E' applicata una gestione della password degli utenti
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Presenza Firewall
- Sono definiti i ruoli e le responsabilità
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del GDPR 2016/679 e della normativa nazionale in vigore

Azienda/Organizzazione **FATEK s.r.l.**

REGISTRO	Registro Fatturazione

SEDE	Sede Operativa Via Lombardi n°8, 10028 Trofarello - TO

Data revisione: 29/04/2019

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato. Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- **finalità del trattamento**, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Titolare trattamento dati	Cognome	De Palo
	Nome	Michele
	E-mail	acquisti@fatek.it
	PEC	fateksrl@legalmail.it
	N° telefono	011 0438596

VALUTAZIONE DEL RISCHIO E MATRICE DI RISCHIO

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	**Improbabile**
2	**Poco probabile**
3	**Probabile**
4	**M. Probabile**
5	**Quasi certo**

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**
5	**Gravissime**

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(*1 ≤ *LR* ≤ 3*)*
Medio - basso	*(*4 ≤ *LR* ≤ 6*)*
Rilevante	*(*8 ≤ *LR* ≤ 12*)*
Alto	*(*15 ≤ *LR* ≤ 25*)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

TRATTAMENTO: Gestione dei Fornitori
Scheda creata in data: 29/04/2019
Ultimo aggiornamento avvenuto in data: 29/04/2019

Struttura	• Sede operativa

Personale coinvolto	
Persone autorizzate	Pozzo Roberta (Dipendente) • Conservazione • Consultazione • Raccolta Del Col Fabio (Dipendente) • Conservazione • Consultazione • Raccolta De Palo Michele (Rappresentante legale) • Conservazione • Consultazione • Raccolta
Partners - Responsabili esterni	Danea Soft s.r.l., p.iva 03365450281 (Azienda Fornitura e Manutenzione Software Gestionale) • Conservazione Credito Valtellinese S.p.A., p.iva 00043260140 (Istituto Bancario) • Conservazione Gruppo IVA Credito Emiliano, p.iva 02823390352 (Istituto Bancario) • Conservazione KLW Consulting s.r.l.s., p.iva 11631640015 (Commercialista) • Conservazione • Consultazione Linuxon di Marengo Piercarlo, p.iva 09347810013 (Società di manutenzione hardware e gestione Server) • Conservazione

Processo di trattamento	
Descrizione	Gestione preventivi da parte di fornitori di materie prime, richiesta fatture, effettuazione pagamenti tramite internet banking.
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Contratto Legge
Finalità del trattamento	Adempimento di obblighi fiscali o contabili Gestione dei fornitori (contratti, ordini, arrivi, fatture) Gestione del contenzioso
Tipo di dati personali	Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Dati bancari per pagamenti
Categorie di interessati	Fornitori
Categorie di destinatari	Banche e istituti di credito Consulenti e liberi professionisti anche in forma associata Responsabili esterni Responsabili interni
Informativa	Si
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario

Frequenza trattamento	Settimanale
Termine cancellazione dati	10 anni
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Pacchetto Office Gestionale Fatturazione
Archiviazione	Armadio chiuso a chiave
Strutture informatiche di archiviazione	
PC 2 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	Del Col Fabio, c.f. DLCFBA72E06L219F (Dipendente)
Note	PC ad uso esclusivo del Sig. Del Col Fabio
Software utilizzati	- Danea Soft - Pacchetto Office
PC 3 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	Pozzo Roberta, c.f. PZZRRT86C66L219C (Dipendente)
Note	PC ad uso esclusivo della Sig.ra Pozzo Roberta
Software utilizzati	- Danea Soft - Pacchetto Office
PC 1 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale)
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	- Danea Soft - Pacchetto Office
Server NAS	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale) Linuxon di Marengo Piercarlo, p.iva 09347810013 (Società di manutenzione hardware e gestione Server)
Note	Server in cui vengono backuppati giornalmente i dati presenti sui PC aziendali. E' dotato di due dischi fissi configurati con la tecnica RAID: ovvero tutto il contenuto che viene memorizzato nel primo disco viene automaticamente copiato anche nel secondo.
Strutture informatiche di backup	
PC 2 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	Del Col Fabio, c.f. DLCFBA72E06L219F (Dipendente)
Note	PC ad uso esclusivo del Sig. Del Col Fabio
Software utilizzati	- Danea Soft - Pacchetto Office
PC 3 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	Pozzo Roberta, c.f. PZZRRT86C66L219C (Dipendente)
Note	PC ad uso esclusivo della Sig.ra Pozzo Roberta
Software utilizzati	- Danea Soft - Pacchetto Office

PC 1 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale)
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	- Danea Soft - Pacchetto Office

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Dispositivi antincendio - Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Sono gestiti i back up - Accesso chiuso a chiave - Accessi limitati alle cartelle di propria competenza. - Presenza Firewall

TRATTAMENTO: Gestione dei Clienti
Scheda creata in data: 29/04/2019
Ultimo aggiornamento avvenuto in data: 29/04/2019

Struttura	• Sede operativa

Personale coinvolto	
Persone autorizzate	Del Col Fabio (Dipendente) • Conservazione • Consultazione • Raccolta De Palo Michele (Rappresentante legale) • Conservazione • Consultazione • Raccolta Pozzo Roberta (Dipendente) • Conservazione • Consultazione • Raccolta
Partners - Responsabili esterni	BRT S.p.A., p.iva 04507990150 (Azienda Trasporto) • Conservazione • Consultazione Corriere Gianotti Autotrasporti di Gianotti Giorgio & C. s.n.c., p.iva 08644220017 (Azienda Trasporto) • Conservazione • Consultazione Credito Valtellinese S.p.A., p.iva 00043260140 (Istituto Bancario) • Conservazione Gruppo IVA Credito Emiliano, p.iva 02823390352 (Istituto Bancario) • Conservazione Danea Soft s.r.l., p.iva 03365450281 (Azienda Fornitura e Manutenzione Software Gestionale) • Conservazione KLW Consulting s.r.l.s., p.iva 11631640015 (Commercialista) • Conservazione • Consultazione • Elaborazione Linuxon di Marengo Piercarlo, p.iva 09347810013 (Società di manutenzione hardware e gestione Server) • Conservazione

Processo di trattamento	
Descrizione	Vengono raccolti e conservati dati relativi a clienti che richiedono le fatture al fine di adempiere agli obblighi fiscali. In particolare vengono richiesti ragione sociale, partita iva ed indirizzo.
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Legge Contratto
Finalità del trattamento	Adempimento di obblighi fiscali o contabili Elaborazione ed invio fatture Gestione del contenzioso
Tipo di dati personali	Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)
Categorie di interessati	Clienti ed utenti

Categorie di destinatari	Consulenti e liberi professionisti anche in forma associata Responsabili esterni Persone autorizzate
Informativa	Si
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Pacchetto Office Gestionale Fatturazione
Archiviazione	Armadio chiuso a chiave
Strutture informatiche di archiviazione	
PC 2 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	Del Col Fabio, c.f. DLCFBA72E06L219F (Dipendente)
Note	PC ad uso esclusivo del Sig. Del Col Fabio
Software utilizzati	- Danea Soft - Pacchetto Office
PC 3 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	Pozzo Roberta, c.f. PZZRRT86C66L219C (Dipendente)
Note	PC ad uso esclusivo della Sig.ra Pozzo Roberta
Software utilizzati	- Danea Soft - Pacchetto Office
PC 1 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale)
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	- Danea Soft - Pacchetto Office
Server NAS	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale) Linuxon di Marengo Piercarlo, p.iva 09347810013 (Società di manutenzione hardware e gestione Server)
Note	Server in cui vengono backuppati giornalmente i dati presenti sui PC aziendali. E' dotato di due dischi fissi configurati con la tecnica RAID: ovvero tutto il contenuto che viene memorizzato nel primo disco viene automaticamente copiato anche nel secondo.

Strutture informatiche di backup	
PC 1 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R (Rappresentante legale)
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	- Danea Soft - Pacchetto Office
PC 2 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	Del Col Fabio, c.f. DLCFBA72E06L219F (Dipendente)
Note	PC ad uso esclusivo del Sig. Del Col Fabio
Software utilizzati	- Danea Soft - Pacchetto Office
PC 3 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	Pozzo Roberta, c.f. PZZRRT86C66L219C (Dipendente)
Note	PC ad uso esclusivo della Sig.ra Pozzo Roberta
Software utilizzati	- Danea Soft - Pacchetto Office

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Dispositivi antincendio - Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi - Le password sono costituite da almeno otto caratteri alfanumerici - L'impianto elettrico è certificato ed a norma - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Sono gestiti i back up - Accesso chiuso a chiave - Accessi limitati alle cartelle di propria competenza. - Presenza Firewall

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

Azienda/Organizzazione **FATEK s.r.l.**

TITOLARE	De Palo Michele
SEDE LEGALE	Sede 1 Via Raffaello Morghen n°35, 10143 Torino - TO

Data revisione: 29/04/2019

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**
5	**Gravissime**

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	**5**	**10**	**15**	**20**	**25**
	4	**4**	**8**	**12**	**16**	**20**
	3	**3**	**6**	**9**	**12**	**15**
	2	**2**	**4**	**6**	**8**	**10**
	1	**1**	**2**	**3**	**4**	**5**
		1	**2**	**3**	**4**	**5**
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ LR ≤ 3)*
Medio - basso	*(4 ≤ LR ≤ 6)*
Rilevante	*(8 ≤ LR ≤ 12)*
Alto	*(15 ≤ LR ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico

4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA – valutazione del rischio normalizzato

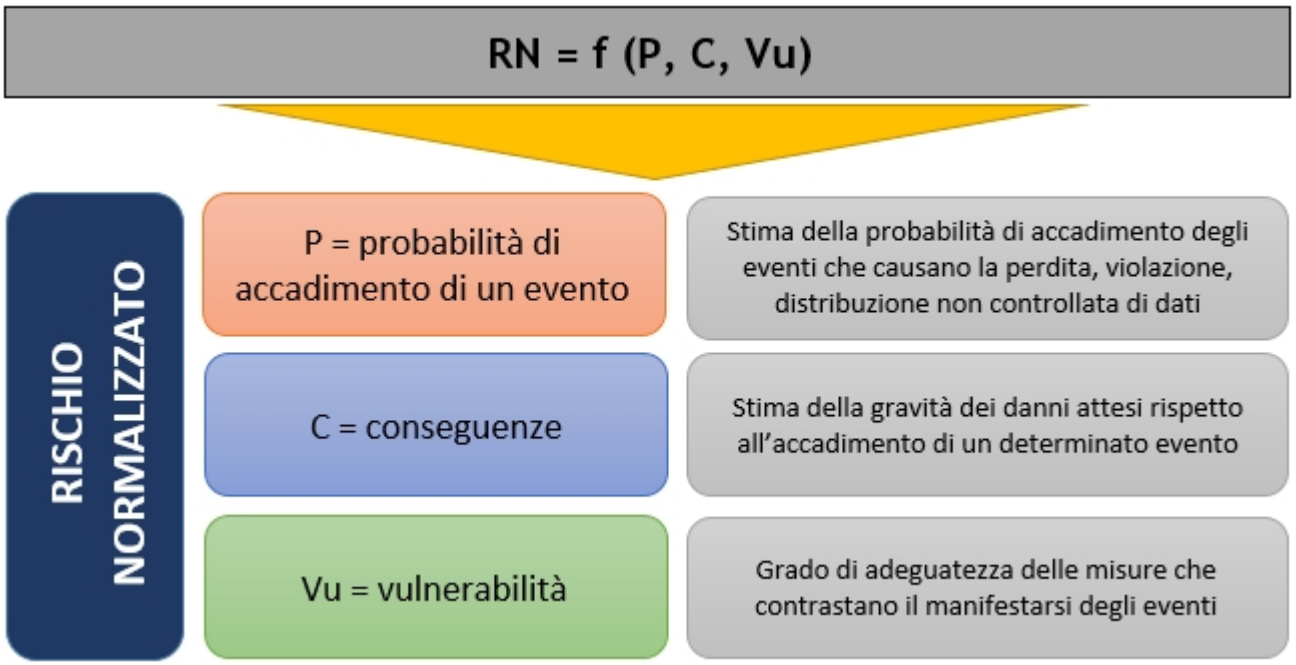
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.
La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

Dove:

P = probabilità
C = conseguenze generate dall'evento



V = vulnerabilità rispetto al grado di adeguatezza delle misure

In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla **probabilità P** è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

PROBABILITÀ	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	**Valori di riferimento**
Molto basso	*(1 ≤ Ri ≤ 2)*
Basso	*(3 ≤ Ri ≤ 4)*
Rilevante	*(6 ≤ Ri ≤ 9)*
Alto	*(12 ≤ Ri ≤ 16)*

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla **Vulnerabilità** (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	**Adeguate**	**0,25**
2	**Parzialmente adeguate**	**0,5**
3	**Inadeguate**	**1**

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	**Valori di riferimento**
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- Gestione del Rapporto di Lavoro

Gestione del Rapporto di Lavoro

Struttura	• Sede operativa

Personale coinvolto	
Titolare del trattamento	De Palo Michele
Persone autorizzate	De Palo Michele, c.f. DPLMHL84P11F335R • Conservazione • Consultazione • Raccolta
Partners - Responsabili esterni	AMJ s.r.l., p.iva 10014130016 • Conservazione • Consultazione • Elaborazione KLW Consulting s.r.l.s., p.iva 11631640015 • Conservazione • Consultazione Wea s.r.l., p.iva 07103660010 • Conservazione • Consultazione • Elaborazione Linuxon di Marengo Piercarlo, p.iva 09347810013 • Conservazione Credito Valtellinese S.p.A., p.iva 00043260140 • Conservazione Gruppo IVA Credito Emiliano, p.iva 02823390352 • Conservazione

Processo di trattamento	
Descrizione	Adempimento degli obblighi previsti dal Contratto di Lavoro o Collaborazione: ad esempio recupero dati per assunzione personale e per emissione buste paga, gestione dei turni lavoro, gestione dei giorni di malattia, ferie, contributi. Adempimento degli obblighi previsti dal D.Lgs 81/08: ad esempio recupero dati per effettuazione corsi di formazione obbligatori in materia di sicurezza sul lavoro, visite Medicina del Lavoro (ove richiesto), ecc.
Fonte dei dati personali	Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	Legge Contratto
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Consenso
Finalità del trattamento	Elaborazione buste paga Contratto di assunzione Bonifici per pagamento stipendio Adempimenti obblighi D.LGS. 81/08 Programmazione delle attività (pianificazione e monitoraggio del lavoro) Gestione del contenzioso

	Gestione dei turni lavoro, gestione dei giorni di malattia, ferie, contributi, ecc.
Tipo di dati personali	Nome e cognome, dati identificativi in generale inclusi residenza, e domicilio; codice fiscale; dati di natura finanziaria quali buste paga, certificati di reddito, IBAN; dati di natura sanitaria quali certificati medici, informazioni in genere circa la salute; informazioni relative a corsi di formazione e titoli di studio acquisiti; dati relativi alla contribuzione previdenziale e all'assicurazione dei lavoratori; dati relativi a fondi di categoria o assicurativi sottoscritti.
Categorie di interessati	Dipendenti o Collaboratori
Categorie di destinatari	Enti pubblici preposti alla Previdenza Sociale, all'Assicurazione dei Lavoratori e all'Accertamento Fiscale(esempio: INPS, INAIL, Agenzia delle Entrate etc.) e qualunque ente pubblico a cui l'azienda è tenuta a fornire i Dati dei propri dipendenti per obbligo di Legge. Enti di Formazione per l'erogazione di corsi di formazione e di aggiornamento professionale dei dipendenti oltreché per i corsi inerenti la sicurezza sul lavoro. Società e Professionisti deputati alla Medicina del Lavoro Società e Professionisti deputati alla gestione, alla manutenzione e all'assistenza da remoto dell'apparato informatico. Professionisti nel settore della Contabilità e della Gestione di Paghe e Contributi. Autorità Giudiziarie competenti.
Informativa	Si
Profilazione	Non necessario
Dati particolari	Non presenti
Consenso minori	Non necessario
Frequenza trattamento	Mensile
Termine cancellazione dati	Sino al termine del rapporto di lavoro o collaborazione con lo studio. Nel caso vengano trattenuti anche Dati Personali soggetti ad obblighi di conservazione stabiliti dalla Legge Italiana od Europea entro e non oltre i limiti dettati dalla normativa di riferimento.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Pacchetto Office
Strutture informatiche di archiviazione	
PC 1 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R
Software utilizzati	- Danea Soft - Pacchetto Office
Server NAS	Struttura interna
Sede di riferimento	Sede Operativa
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R Linuxon di Marengo Piercarlo, p.iva 09347810013

Strutture informatiche di backup	
PC 1 - Ufficio Operativo	Struttura interna
Sede di riferimento	Sede Operativa
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	- Danea Soft - Pacchetto Office

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Limitate	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Accessi limitati alle cartelle di propria competenza.
- Dispositivi antincendio
- E' applicata una gestione della password degli utenti
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- L'impianto elettrico è certificato ed a norma
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Presenza Firewall
- Sono definiti i ruoli e le responsabilità
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Viene eseguita opportuna manutenzione

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Accessi limitati alle cartelle di propria competenza.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Dispositivi antincendio	• Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
E' applicata una gestione della password degli utenti	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
L'impianto elettrico è certificato ed a norma	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Presenza Firewall	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	• Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	Adeguate

	• Agenti fisici (incendio, allagamento, attacchi esterni)	
Sono utilizzati software antivirus e anti intrusione	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Limitate	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Vulnerabilità - Vu**	**Rischio normalizzato - RN**
Rilevante	0,25	Basso

A valle della DPIA l'attività risulta a rischio **Basso**

VALUTAZIONE ARCHIVI INFORMATICI

Azienda/Organizzazione **FATEK s.r.l.**

SEDE LEGALE	Sede 1 Via Raffaello Morghen n°35, 10143 Torino - TO

Data revisione: 29/04/2019

VALUTAZIONE ARCHIVI INFORMATICI

Di seguito, è riportata la valutazione degli archivi informatici in dotazione all'organizzazione.
L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ LR ≤ 3)*
Medio - basso	*(4 ≤ LR ≤ 6)*
Rilevante	*(8 ≤ LR ≤ 12)*
Alto	*(15 ≤ LR ≤ 25)*

RISULTATI

Nome	PC 1 - Ufficio Operativo
Tipo Struttura	Interna
Sede	Sede Operativa (Trofarello)
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R
Note	PC ad uso esclusivo del Sig. De Palo Michele
Software utilizzati	• Danea Soft - Software gestionale • Pacchetto Office

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Dispositivi antincendio • Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Viene eseguita opportuna manutenzione • Sono utilizzati software antivirus e anti intrusione • Sono gestiti i back up • Accesso chiuso a chiave • Accesso Personalizzato al software gestionale

Nome	PC 2 - Ufficio Operativo
Tipo Struttura	Interna
Sede	Sede Operativa (Trofarello)
Personale con diritti di accesso	Del Col Fabio, c.f. DLCFBA72E06L219F
Note	PC ad uso esclusivo del Sig. Del Col Fabio
Software utilizzati	• Danea Soft - Software gestionale • Pacchetto Office

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Dispositivi antincendio • Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Viene eseguita opportuna manutenzione • Sono utilizzati software antivirus e anti intrusione • Sono gestiti i back up • Accesso chiuso a chiave • Accesso Personalizzato al software gestionale

Nome	**PC 3 - Ufficio Operativo**
Tipo Struttura	Interna
Sede	Sede Operativa (Trofarello)
Personale con diritti di accesso	Pozzo Roberta, c.f. PZZRRT86C66L219C
Note	PC ad uso esclusivo della Sig.ra Pozzo Roberta
Software utilizzati	• Danea Soft - Software gestionale • Pacchetto Office

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Dispositivi antincendio • Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi • Le password sono costituite da almeno otto caratteri alfanumerici • L'impianto elettrico è certificato ed a norma • Viene eseguita opportuna manutenzione • Sono utilizzati software antivirus e anti intrusione • Sono gestiti i back up • Accesso chiuso a chiave • Accesso Personalizzato al software gestionale

Nome	**Server NAS**
Tipo Struttura	Interna
Sede	Sede Operativa (Trofarello)
Personale con diritti di accesso	De Palo Michele, c.f. DPLMHL84P11F335R Linuxon di Marengo Piercarlo, p.iva 09347810013
Note	Server in cui vengono backuppati giornalmente i dati presenti sui PC aziendali. E' dotato di due dischi fissi configurati con la tecnica RAID: ovvero tutto il contenuto che viene memorizzato nel primo disco viene automaticamente copiato anche nel secondo.

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO		
Probabilità	**Conseguenza**	**Livello di rischio**
Poco probabile	Marginali	Medio-basso

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
• Dispositivi antincendio • Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi • L'impianto elettrico è certificato ed a norma • Accessi limitati alle cartelle di propria competenza. • Viene eseguita opportuna manutenzione • Presenza Firewall

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

INDICE

PREMESSA

L'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. La **FATEK s.r.l.** ha adottato una procedura interna diretta ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.

1. UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato al dipendente è uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata.

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio, in caso di prolungata assenza o impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno previa autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*, in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal *Responsabile dei sistemi informatici* della **FATEK s.r.l.**. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo autorizzazione esplicita del *Responsabile dei sistemi informatici aziendali*.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione,

comunicazione o altro (come ad esempio masterizzatori, modem, ecc.), se non con l'autorizzazione espressa del *Responsabile dei sistemi informatici aziendali.*
Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il *Responsabile dei sistemi informatici aziendali* nel caso in cui vengano rilevati virus.

2. UTILIZZO DELLA RETE

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
Il *Responsabile dei sistemi informatici aziendali* può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.
Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3. GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal*l Responsabile dei sistemi informatici aziendali.*
È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati particolari (ex dati sensibili) e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al *Responsabile dei sistemi informatici aziendali. (n.b.: in molti sistemi la comunicazione di variazione può essere "generata" dallo stesso sistema informatico all'atto della modifica, con invio di e-mail automatica al Responsabile; molti sistemi permettono di "temporizzare" la validità delle password e, quindi, di bloccare l'accesso al personale computer e/o al sistema, qualora non venga autonomamente variata dall'incaricato entro i termini massimi: in questi casi vanno adattate le istruzioni contenute nel presente regolamento)*
Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.
La password deve essere immediatamente sostituita, dandone comunicazione al *Responsabile dei sistemi informatici aziendali*, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia alla Direzione o al *Responsabile dei sistemi informatici aziendali*.

4. UTILIZZO DEI SUPPORTI MAGNETICI

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati particolari (ex dati sensibili) e giudiziari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione.
I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

5. UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i Pc connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
I PC portatili utilizzati all'esterno (convegni, visite in azienda, ecc), in caso di allontanamento, devono essere custoditi in un luogo protetto.

6. USO DELLA POSTA ELETTRONICA

La casella di posta, assegnata dall'Azienda all'utente, è uno **strumento di lavoro**. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per la **FATEK s.r.l.** deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto, e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).
Per la trasmissione di file all'interno della **FATEK s.r.l.** è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati.
È obbligatorio controllare i file attachements di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
È vietato inviare catene telematiche (o di Sant'Antonio). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al *Responsabile dei sistemi informatici aziendali*. Non si devono in alcun caso attivare gli allegati di tali messaggi.

7. USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI

Il PC abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal *Responsabile dei sistemi informatici aziendali*.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

8. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

9. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

Data 26/03/2019

La Direzione

ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

INDICE

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali della **FATEK s.r.l.**, conformemente al Regolamento (Ue) 2016/679 (GDPR) ed alla normativa nazionale in vigore. I dipendenti, i collaboratori, i consulenti, i volontari ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza. Ogni utilizzo dei dati in possesso dell'Azienda diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo e all'immagine dell'Azienda.

1. DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR) e la normativa nazionale in vigore, si definisce:

- Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- Violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

2. ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR) e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli aziendali e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

3. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI

Le principali operazioni degli incaricati del trattamento sono:

- identificazione dell'interessato:

al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni;

- verifica del controllo dell'esattezza del dato e della corretta digitazione:

al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento;

- Norme logistiche per l'accesso fisico ai locali:

I locali, ove sono custoditi i dati personali (ed in particolare quelli di natura sensibile), devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere conosciuti o accessibili da parte di soggetti non autorizzati. Si raccomanda, in caso di allontanamento dal proprio ufficio o dalla propria postazione di lavoro, di adottare tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'organizzazione di appartenenza. Laddove si esegue il trattamento di Dati Personali, deve essere possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti tali dati. Pertanto le porte degli uffici ed almeno un armadio per ufficio devono essere dotati di serratura con chiave. Al termine dell'orario lavorativo, ove la dinamica delle attività ed il numero di occupanti lo consentano, è necessario chiudere sempre a chiave gli uffici nei quali vengono svolti trattamenti di Dati Personali.

4. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

a) Gestione strumenti elettronici (pc fissi e portatili)

Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.

Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;

• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;

• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:

- Non deve mai essere disattivato;
- Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
- Deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;

• Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.

Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:

• prima della riconsegna, rimuovere eventuali file ivi elaborati;

• quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli

appositi cavi in acciaio dotati di lucchetto;
• quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
• in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b) Gestione username e password

L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:
• tutela l'utilizzatore ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
• è necessario per gestire correttamente gli accessi a risorse condivise.
Ciascun incaricato deve scegliere le password in base ai seguenti criteri:
• devono essere lunghe almeno otto caratteri;
• non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
• devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
• non deve essere uguali alle precedenti.
Per la corretta gestione della password è necessario:
• Ogni password ricevuta va modificata al primo utilizzo;
• La password venga conservata in un luogo sicuro;
• Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
• Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

c) Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Responsabile del trattamento per i Sistemi Elettronici. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:
• Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
• Non installare sistemi per connessione esterne (es: modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
• Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
• Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.
Si ricorda che normalmente la condivisione di aree e di risorse del proprio PC è vietata. Può essere autorizzata dal Servizio Informatico, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

d) Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore o del volontario che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza dell'azienda e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:
• Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
• È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
• La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione.
Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
• l'indirizzo del destinatario sia stato correttamente digitato,
• l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
• nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

e) Gestione del salvataggio dei dati

Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni

f) Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del servizio Sistemi. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

g) Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Azienda è stato installato un software antivirus aziendale che si aggiorna automaticamente all'ultima versione disponibile.
L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al responsabile del Servizio Informatico.
Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.

5. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o giudiziari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.

Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari (ex dati sensibili) e/o giudiziari, il rispetto di queste norme è obbligatorio.

a) distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:

- la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;
- la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

c) Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
- i supporti devono essere archiviati in ambiente ad accesso controllato;
- i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.
- è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

6. ADDETTI ALLA MANUTENZIONE

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici:

• Effettuare operazioni di manutenzione e supporto per verifica corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;

• gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione dell'Amministratore di sistema;

• gestire i profili di autorizzazione degli incaricati al trattamento dei dati, su specifiche impartite dai responsabili di funzione/BU, su indicazione dell'Amministratore di sistema;

• provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica dei responsabili ovvero della Direzione Risorse Umane e su indicazione dell'Amministratore di sistema;

• custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali;

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.

A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le seguenti istruzioni operative:

• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.

• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.

• Per effettuare operazioni di manutenzione sui database aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.

• Devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;

• E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.

• Tutti i dati personali contenuti nei data base devono essere protetti da password;

• Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

o in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;

o in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.

• Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;

• L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;

• Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;

• l'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;

• E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;

• Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

7. OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

8. NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

Data 26/03/2019

La Direzione

ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016** (**GDPR**) e la normativa nazionale in vigore, impone al titolare del trattamento di notificare all'autorità di controllo la violazione di dati personali (**data breach**) entro 72 ore dal momento in cui ne viene a conoscenza.

L'obbligo di notifica scatta se la violazione, ragionevolmente, comporta un rischio per i diritti e le libertà delle persone fisiche, qualora, poi, il rischio fosse elevato, allora, oltre alla notifica, il titolare è tenuto a darne comunicazione all'interessato.

Il termine per adempiere alla notifica è brevissimo, 72 ore dal momento in cui il titolare ne viene a conoscenza, mentre, l'eventuale comunicazione agli interessati, deve essere fatta senza indugio.

L'eventuale ritardo nella notificazione deve essere giustificato, il mancato rispetto dell'obbligo di notifica, invece, pone l'autorità di controllo nella condizione di applicare le misure correttive a sua disposizione ovvero: l'esercizio dei poteri previsti dall'art.58 GDPR (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati), la imposizione di sanzioni amministrative secondo l'art. 83 GDPR e della normativa nazionale in vigore.

Per **"Violazione di dati**" si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (Art. 4 p.12 del GDPR).

La violazione di dati è un particolare tipo di incidente di sicurezza, per effetto del quale, il titolare non è in grado di garantire il rispetto dei principi prescritti dall'art. 5 del GDPR per il trattamento dei dati personali.

Preliminarmente, dunque, il titolare deve poter identificare l'incidente di sicurezza in genere, quindi, comprendere che l'incidente ha impatto sulle informazioni e, infine, che tra le informazioni coinvolte dall'incidente vi sono dati personali.

L'art. 33 p.5 del GDPR prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

L'art. 33 p.2 GDPR prevede espressamente il dovere per il responsabile, quando viene a conoscenza di una violazione, di informare, senza ingiustificato ritardo, il titolare.

E' importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono le 72 ore per la notifica.

Si possono distinguere tre tipi di violazioni:

1. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
2. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
3. violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

Una violazione potrebbe comprendere una o più tipologie.

Per comprendere quando notificare la violazione è opportuno effettuare una valutazione dell'entità dei rischi:

- **Rischio assente**: la notifica al Garante non è obbligatoria.
- **Rischio presente**: è necessaria la notifica al Garante.

- **Rischio elevato**: In presenza di rischi "elevati", è necessaria la comunicazione agli interessati. Nel momento in cui il titolare del trattamento adotta sistemi di crittografia dei dati, e la violazione non comporta l'acquisizione della chiave di decrittografia, la comunicazione ai soggetti interessati non sarà un obbligo.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (es. dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (es. rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (es. pazienti, minori, soggetti indagati).

Per la notifica della violazione e la comunicazione al Garante occorre compilare gli appositi moduli messi a disposizione.

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

A seguito del recepimento della direttiva 2009/136/Ce ad opera del decreto legislativo 28 maggio 2012, n. 69, i fornitori di servizi di comunicazione elettronica sono oggi tenuti a comunicare al Garante e, in alcuni casi, al contraente o ad altre persone interessate, le violazioni dei dati personali (Data breach) che detengono nell'ambito delle proprie strutture.

Titolare che effettua la comunicazione

Denominazione o ragione sociale: ……

Provincia……Comune……

Cap. …… Indirizzo ……

Nome persona fisica addetta alla comunicazione……

Cognome persona fisica addetta alla comunicazione……

Funzione rivestita……

Indirizzo Email/PEC per eventuali comunicazioni……

Recapito telefonico per eventuali comunicazioni……

Eventuali Contatti (altre informazioni) ……

Natura della comunicazione

☐ Nuova comunicazione

☐ Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)

☐ Ritiro precedente comunicazione

Breve descrizione del trattamento di dati personali

Quando si è verificata la violazione di dati personali?

☐ Il……

☐ Tra il…… e il ……

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)

☐ Copia (i dati sono ancora presenti sui sistemi del titolare)

☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

☐ Altro: ……

Dispositivo oggetto della violazione

☐ Postazione di lavoro

☐ Dispositivo di acquisizione o dispositivo-lettore

☐ Smart card o analogo supporto portatile

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Rete

☐ Altro: ……

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione di dati personali?

☐ N. …… di persone

☐ Circa …… persone

☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono coinvolti nella violazione ?

☐ Dati anagrafici

☐ Numero di telefono (fisso o mobile)

☐ Indirizzo di posta elettronica

☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)

☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

☐ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari Ancora sconosciuto

☐ Altro: ……

Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il ……

☐ No, perché ……

Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?

Quale canale è utilizzato per la comunicazione ai contraenti (o alle persone interessate)?

Quali misure tecnologiche ed organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

La violazione coinvolge contraenti (o altre figure interessate) che si trovano in altri Paesi UE?

☐ Sì

☐ No

La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?

☐ No

☐ Sì

VIOLAZIONE DI DATI PERSONALI
MODELLO DI COMUNICAZIONE AL GARANTE

Secondo quanto prescritto dal **Provvedimento del 4 giugno 2015 "***Linee guida in materia di dossier sanitario***"**, i titolari di trattamento dei dati personali effettuati mediante il *dossier* sanitario sono tenuti a comunicare al Garante all'indirizzo: **databreach.dossier@pec.gpdp.it** le violazioni dei dati personali (*data breach*) che si verificano nell'ambito delle proprie strutture (*cfr. punto 7.1. delle predette Linee guida*).

La comunicazione deve essere effettuata entro 48 ore dalla conoscenza del fatto, compilando il modulo che segue.

Titolare del trattamento del dossier sanitario

Denominazione o ragione sociale: ……

Provincia……Comune……

Cap. …… Indirizzo ……

Nome persona fisica addetta alla comunicazione……

Cognome persona fisica addetta alla comunicazione……

Funzione rivestita……

Indirizzo PEC e/o EMAIL per eventuali comunicazioni……

Recapito telefonico per eventuali comunicazioni……

Eventuali Contatti (altre informazioni) ……

Natura della comunicazione

……

……

……

Breve descrizione della violazione dei dati personali trattati mediante il *dossier* sanitario

Quando si è verificata la violazione dei dati personali trattati mediante il *dossier* sanitario?

☐ Il……

☐ Tra il…… e il ……

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)

☐ Copia (i dati sono ancora presenti sui sistemi del titolare)

☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

☐ Altro: ……

Dispositivo oggetto della violazione

☐ Computer

☐ Rete

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Documento cartaceo

☐ Altro: ……

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

☐ N. …… di persone

☐ Circa …… persone

☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

☐ Dati anagrafici

☐ Indirizzo di posta elettronica

☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)

☐ Dati idonei a rivelare lo stato di salute

☐ Dati relativi a minori

☐ Dati sanitari relativi a persone sieropositive, a donne che si sono sottoposte a un'interruzione volontaria di gravidanza, a vittime di atti di violenza sessuale o di pedofilia, a persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, a donne che hanno deciso di partorire in anonimato, i dati riferiti ai servizi offerti dai consultori familiari

☐ Copie per immagine su supporto informatico di documenti analogici

☐ Ancora sconosciuto

☐ Altro: ……

Livello di gravità della violazione dei dati personali trattati mediante il *dossier* sanitario (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il ……

☐ No, perché ……

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

INFORMATIVA LAVORATORI DIPENDENTI

La scrivente Società **FATEK s.r.l.** comunica che, per l'instaurazione e la gestione del rapporto di lavoro in corso, è titolare di dati Suoi e dei Suoi familiari(1) qualificati come dati personali ai sensi del Regolamento 2016/679 e della normativa nazionale in vigore.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1. La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:
   - Mista - elettronica e cartacea
2. I dati raccolti vengono utilizzati per le seguenti finalità:
   - Adempimenti obblighi D.LGS. 81/08
   - Bonifici per pagamento stipendio
   - Contratto di assunzione ed elaborazione buste paga
   - Gestione dei turni lavoro, gestione dei giorni di malattia, ferie, contributi, ecc.
   - Gestione del contenzioso
   - Programmazione delle attività (pianificazione e monitoraggio del lavoro)

BASE GIURIDICA

3. Le basi giuridiche su cui si fonda il trattamento per i dati comuni, secondo l'Art.6 del Regolamento GDPR, sono:
   - Legge e Contratto;

La base giuridica su cui si fonda il trattamento per categorie particolari di dati personali, secondo l'Art.9 del Regolamento GDPR, è:

- Consenso;

Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti.

La società tratta i dati facoltativi degli utenti in base al consenso, ossia mediante l'approvazione esplicita della presente policy privacy e in relazione alle modalità e finalità di seguito descritte.

CATEGORIE DI DESTINATARI

4. Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati in Italia esclusivamente per le finalità sopra specificate a:
   - Autorità Giudiziarie competenti.;
   - Enti di Formazione per l'erogazione di corsi di formazione e di aggiornamento professionale dei dipendenti oltreché per i corsi inerenti la sicurezza sul lavoro.;
   - Enti pubblici preposti alla Previdenza Sociale, all'Assicurazione dei Lavoratori e all'Accertamento Fiscale(esempio: INPS, INAIL, Agenzia delle Entrate etc.) e qualunque ente pubblico a cui l'azienda è tenuta a fornire i Dati dei propri dipendenti per obbligo di Legge.;
   - Professionisti nel settore della Contabilità e della Gestione di Paghe e Contributi.;
   - Società e Professionisti deputati alla gestione, alla manutenzione e all'assistenza da remoto dell'apparato informatico.;
   - Società e Professionisti deputati alla Medicina del Lavoro;

Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi oltre che il Rappresentante Legale dell'azienda il Sig. De Palo Michele anche tutte le persone autorizzate e tutti i responsabili esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati. L'elenco completo delle persone interne o esterne all'azienda che potranno venire a conoscenza dei suoi dati è disponibile a richiesta.

5. In relazione al rapporto di lavoro, l'azienda potrà trattare dati che la legge definisce "particolari" in quanto idonei a rilevare ad esempio:
   a) lo stato generale di salute (assenze per malattia, maternità, infortunio o l'avviamento obbligatorio) idoneità o meno a determinate mansioni (quale esito espresso da personale medico a seguito di visite mediche preventive/periodiche o richieste da Lei stesso/a);
   b) l'adesione ad un sindacato (assunzione di cariche e/o richiesta di trattenute per quote di associazione sindacale), l'adesione ad un partito politico o la titolarità di cariche pubbliche elettive (permessi od aspettativa), convinzioni religiose (festività religiose fruibili per legge);

I dati di natura particolare, concernenti lo stato di salute, che tratta il medico competente nell'espletamento dei compiti previsti dal D.Lgs. 81/08 e dalle altre disposizioni in materia di salute e sicurezza sui luoghi di lavoro, per l'effettuazione degli accertamenti medici preventivi e periodici, verranno trattati presso il datore di lavoro esclusivamente dallo stesso medico quale Responsabile del trattamento del trattamento, per il quale la società chiede espresso consenso.

DIRITTI DELL'INTERESSATO

Relativamente ai dati medesimi si potranno esercitare i diritti previsti dagli artt. 15 - "Diritto di accesso dell'interessato", 16 - "Diritto di rettifica", 17 - "Diritto alla cancellazione", 18 – "Diritto di limitazione al trattamento", 20 – "Diritto alla portabilità dei dati" del **Regolamento UE 2016/679** e normativa nazionale in vigore, nei limiti ed alle condizioni previste dall'art. 12 del Regolamento stesso.

PERIODO DI CONSERVAZIONE

Sino al termine del rapporto di lavoro o collaborazione con l'azienda. Nel caso vengano trattenuti anche Dati Personali soggetti ad obblighi di conservazione stabiliti dalla Legge Italiana od Europea entro e non oltre i limiti dettati dalla normativa di riferimento.

6. Titolare del trattamento dei Suoi dati personali è FATEK s.r.l., p.iva 10786800010, c.f. 10786800010
   - Email: info@fatek.it
   - PEC: fateksrl@legalmail.it
   - Telefono: 011 0438596

Data Timbro e firma azienda

****

Il/La sottoscritto/a _____ dichiara di aver ricevuto completa informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 e della normativa nazionale in vigore, ed esprime il consenso al trattamento ed alla comunicazione dei propri dati personali con particolare riguardo a quelli cosiddetti particolari nei limiti, per le finalità e per la durata precisati nell'informativa.

Data Firma

(1)

COGNOME	NOME	REL. DI PARENTELA	FIRMA
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....
.....	.....	.....	.....

(1) Da inserire quando si trattano anche dati relativi ai familiari (ad esempio assegni per il nucleo familiare, permessi per assistenza ai familiari, ecc.). Il consenso deve essere sottoscritto dai familiari maggiorenni.

Data Firma

INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI - CLIENTI

I dati personali dell'utente sono utilizzati dalla **FATEK s.r.l.**, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e della normativa nazionale in vigore.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1. La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:
   - Mista - elettronica e cartacea

   con le seguenti finalità:
   - Adempimento di obblighi fiscali o contabili
   - Elaborazione ed invio fatture
   - Gestione del contenzioso

BASE GIURIDICA

2. Le basi giuridiche su cui si fonda il trattamento per i dati comuni, secondo l'Art.6 del Regolamento GDPR, sono:
   - Legge;
   - Contratto;

   Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti.

CATEGORIE DI DESTINATARI

3. Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di destinatari:
   - Consulenti e liberi professionisti anche in forma associata;
   - Persone autorizzate;
   - Responsabili esterni;

   Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi oltre che il Rappresentante Legale dell'azienda il Sig. De Palo Michele anche tutte le persone autorizzate e tutti i responsabili esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati. L'elenco completo delle persone interne o esterne all'azienda che potranno venire a conoscenza dei suoi dati è disponibile a richiesta.

PERIODO DI CONSERVAZIONE

I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.

DIRITTI DELL'INTERESSATO

4. Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale in vigore, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:
   - richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso dell'interessato – art. 15 del Regolamento 679/2016);
   - conoscerne l'origine;
   - riceverne comunicazione intelligibile;
   - avere informazioni circa la logica, le modalità e le finalità del trattamento;
   - richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti (diritto di rettifica e cancellazione – artt. 16 e 17 del Regolamento 679/2016);
   - diritto di limitazione e/o di opposizione al trattamento dei dati che lo riguardano (art. 18 del Regolamento 679/2016);
   - diritto di revoca;
   - diritto alla portabilità dei dati (art. 20 del Regolamento 679/2016);
   - nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
   - il diritto di presentare un reclamo all'Autorità di controllo (diritto di accesso dell'interessato – art. 15 del Regolamento 679/2016).
5. Titolare del trattamento dei Suoi dati personali è FATEK s.r.l., p.iva 10786800010, c.f. 10786800010
   - Email: info@fatek.it
   - PEC: fateksrl@legalmail.it
   - Telefono: 011 0438596

INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI - FORNITORI

I dati personali dell'utente sono utilizzati dalla **FATEK s.r.l.**, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679 e della normativa nazionale in vigore.

MODALITÀ E FINALITÀ DEL TRATTAMENTO DATI

1. La informiamo che i dati verranno trattati con il supporto dei seguenti mezzi:
   - Mista - elettronica e cartacea

   con le seguenti finalità:
   - Adempimento di obblighi fiscali o contabili
   - Gestione dei fornitori (contratti, ordini, arrivi, fatture)
   - Gestione del contenzioso

BASE GIURIDICA

2. Le basi giuridiche su cui si fonda il trattamento per i dati comuni, secondo l'Art.6 del Regolamento GDPR, sono:
   - Legge;
   - Contratto;

   Il conferimento dei dati è obbligatorio per tutto quanto è richiesto dagli obblighi legali e contrattuali e pertanto l'eventuale rifiuto a fornirli in tutto o in parte può dar luogo all'impossibilità di fornire i servizi richiesti.

CATEGORIE DI DESTINATARI

3. Ferme restando le comunicazioni eseguite in adempimento di obblighi di legge e contrattuali, tutti i dati raccolti ed elaborati potranno essere comunicati esclusivamente per le finalità sopra specificate alle seguenti categorie di destinatari:
   - Banche e istituti di credito;
   - Consulenti e liberi professionisti anche in forma associata;
   - Responsabili esterni;
   - Responsabili interni;

   Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi oltre che il Rappresentante Legale dell'azienda il Sig. De Palo Michele anche tutte le persone autorizzate e tutti i responsabili esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati. L'elenco completo delle persone interne o esterne all'azienda che potranno venire a conoscenza dei suoi dati è disponibile a richiesta.

PERIODO DI CONSERVAZIONE

Il periodo di conservazione dei dati è: 10 anni

DIRITTI DELL'INTERESSATO

4. Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale in vigore, l'interessato può, secondo le modalità e nei limiti previsti dalla vigente normativa, esercitare i seguenti diritti:
   - richiedere la conferma dell'esistenza di dati personali che lo riguardano (diritto di accesso dell'interessato – art. 15 del Regolamento 679/2016);
   - conoscerne l'origine;
   - riceverne comunicazione intelligibile;
   - avere informazioni circa la logica, le modalità e le finalità del trattamento;
   - richiederne l'aggiornamento, la rettifica, l'integrazione, la cancellazione, la trasformazione in forma anonima, il blocco dei dati trattati in violazione di legge, ivi compresi quelli non più necessari al perseguimento degli scopi per i quali sono stati raccolti (diritto di rettifica e cancellazione – artt. 16 e 17 del Regolamento 679/2016);
   - diritto di limitazione o di opposizione al trattamento dei dati che lo riguardano (art. 18 del Regolamento 679/2016);
   - diritto di revoca;
   - diritto alla portabilità dei dati (art. 20 del Regolamento 679/2016);
   - nei casi di trattamento basato su consenso, ricevere i propri dati forniti al titolare, in forma strutturata e leggibile da un elaboratore di dati e in un formato comunemente usato da un dispositivo elettronico;
   - il diritto di presentare un reclamo all'Autorità di controllo (diritto di accesso dell'interessato – art. 15 del Regolamento 679/2016).
5. Titolare del trattamento dei Suoi dati personali è FATEK s.r.l., p.iva 10786800010, c.f. 10786800010
   - Email: info@fatek.it
   - PEC: fateksrl@legalmail.it
   - Telefono: 011 0438596

Lettera di incarico

Torino, 26/03/2019

Oggetto: Lettera di nomina quale persona autorizzata al trattamento dati

Il sottoscritto **De Palo Michele**, c.f. DPLMHL84P11F335R, rappresentante legale della **FATEK s.r.l.,** con sede legale in Via Raffaello Morghen n°35, 10143 Torino (TO), **conferisce** al Sig. **Del Col Fabio**, c.f. DLCFBA72E06L219F, per la sede Operativa, Via Lombardi n°8, 10028 Trofarello (TO), dalla data del 26/03/2019, l'**incarico** di compiere le operazioni di trattamento di seguito elencate, con l'avvertimento che dovrà operare osservando le direttive del *titolare*.

A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal *titolare/responsabile*;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
    a) divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del *titolare/responsabile*;
    b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
    c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Lettera di incarico

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME CONTATTO/PERSONA AUTORIZZATA

Sede Operativa
Registro Fatturazione

- Gestione dei Fornitori
  - Conservazione
  - Consultazione
  - Raccolta

Registro Fatturazione

- Gestione dei Clienti
  - Conservazione
  - Consultazione
  - Raccolta

FORMAZIONE
Con l'accettazione del presente documento, si attesta l'avvenuta frequenza del corso di formazione e la conoscenza delle basi del Regolamento Generale sulla Protezione dei Dati Personali 2016/679.

Per conoscenza ed accettazione Persona autorizzata al trattamento dati (Fabio Del Col)	Il titolare del trattamento (Michele De Palo)
_____ (firma)	_____ (firma)

Lettera di incarico

Torino, 26/03/2019

Oggetto: Lettera di nomina quale persona autorizzata al trattamento dati

Il sottoscritto **De Palo Michele**, c.f. DPLMHL84P11F335R, rappresentante legale della **FATEK s.r.l.**, con sede legale in Via Raffaello Morghen n°35, 10143 Torino (TO), **conferisce** alla Sig.ra **Pozzo Roberta**, c.f. PZZRRT86C66L219C, per la Sede Operativa, Via Lombardi n°8, 10028 Trofarello (TO), dalla data del 26/03/2019, l'**incarico** di compiere le operazioni di trattamento di seguito elencate, con l'avvertimento che dovrà operare osservando le direttive del *titolare*.

A tal fine, vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal *titolare/responsabile*;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
    a) divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del *titolare/responsabile*;
    b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
    c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Lettera di incarico

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME CONTATTO/PERSONA AUTORIZZATA

Sede Operativa
Registro Fatturazione
- Gestione dei Fornitori
  - Conservazione
  - Consultazione
  - Raccolta

Registro Fatturazione
- Gestione dei Clienti
  - Conservazione
  - Consultazione
  - Raccolta

FORMAZIONE
Con l'accettazione del presente documento, si attesta l'avvenuta frequenza del corso di formazione e la conoscenza delle basi del Regolamento Generale sulla Protezione dei Dati Personali 2016/679.

Per conoscenza ed accettazione Persona autorizzata al trattamento dati (Roberta Pozzo)	Il titolare del trattamento (Michele De Palo)
_____ (firma)	_____ (firma)

Lettera di incarico

Torino, 26/03/2019

Oggetto: Lettera di nomina al Responsabile esterno del trattamento dati

Il sottoscritto De Palo Michele, c.f. DPLMHL84P11F335R, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e della normativa nazionale in vigore,

NOMINA

KLW Consulting s.r.l.s., p.iva 11631640015 Responsabile esterno del trattamento dei dati per la sede Operativa, Via Lombardi n°8, 10028 Trofarello (TO), dalla data del 26/03/2019, con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate.
In qualità di Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonchè le istruzioni impartite dal Titolare.

REQUISITI DELL'INCARICO

MATERIA DISCIPLINATA	Consulenza Contabile
DURATA DEL TRATTAMENTO	• I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
DESCRIZIONE DEI TRATTAMENTI	I dati vengono trattati al fine di elaborare la contabilità aziendale. In particolare questo responsabile esterno esegue le registrazioni contabili, gestisce le operazioni fiscali e previdenziali, redige il bilancio di esercizio, elabora i resoconti sulla situazione fiscale aziendale, gestisce per conto dell'azienda le relazioni con l'Agenzia delle entrate nel caso di divergenze di dati.
FINALITÀ	• Attività di consulenza • Elaborazione dati contabili
TIPO DI DATI PERSONALI	• Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) • Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)
CATEGORIE DI INTERESSATI	• Clienti • Dipendenti • Fornitori
DESTINAZIONE DEI DATI ALLA CONCLUSIONE DEL CONTRATTO	Cancellazione dei dati

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME PARTNER

Il soggetto nominato avrà il compito di trattare i dati personali riferiti alle seguenti attività di trattamento, in cui è coinvolto come partner:

Sede Operativa
Registro Dipendenti

- Gestione del Rapporto di Lavoro
  - Conservazione
  - Consultazione

Sede Operativa
Registro Fatturazione

- Gestione dei Fornitori
  - Conservazione
  - Consultazione

Sede Operativa
Registro Fatturazione

- Gestione dei Clienti
  - Conservazione
  - Consultazione
  - Elaborazione

COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

in applicazione del considerando art. 28 del Regolamento UE 2016/679 e della normativa nazionale in vigore

PRINCIPI GENERALI DA OSSERVARE

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale e per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
  - secondo il principio di liceità, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
  - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- i dati devono essere raccolti solo per scopi:
  - determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
  - espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
  - legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
  - compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;
- i dati devono, inoltre, essere:
  - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
  - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
  - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì

di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
- non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
- conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare, come previsto dall'art.28 e dall'art.30 comma 2 del Regolamento GDPR:

a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
b) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
   - il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
   - le categorie dei trattamenti effettuati;
   - se del caso, i trasferimenti di dati personali verso Paesi terzi;
   - descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;
c) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;
e) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
f) adempiere agli obblighi di sicurezza, quali:
   - adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - definire una politica di sicurezza per assicurare su base permanente la

riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
- assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
h) su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
i) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;
j) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
k) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;
l) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.
m) dare riscontro preventivo dell'eventuale trasferimento dei dati verso paesi extra UE, la cui normativa non è equiparabile a quella Europea, applicando preventivamente garanzie adeguate a tale trasferimento;
n) ricorrere ad un altro responsabile, per gestire attività di trattamento specifiche, solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento (articolo 28 comma 2 Regolamento GDPR).

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.
L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.
Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico
Il Responsabile del trattamento
(KLW Consulting s.r.l.s.)

_____
(firma)

Il titolare del trattamento
(Michele De Palo)

_____
(firma)

Lettera di incarico

Torino, 26/03/2019

Oggetto: Lettera di nomina al Responsabile esterno del trattamento dati

Il sottoscritto De Palo Michele, c.f. DPLMHL84P11F335R, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e della normativa nazionale in vigore,

NOMINA

AMJ s.r.l., p.iva 10014130016 Responsabile esterno del trattamento dei dati per la sede Operativa, Via Lombardi n°8, 10028 Trofarello (TO), dalla data del 26/03/2019, con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate.
In qualità di Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonchè le istruzioni impartite dal Titolare.

REQUISITI DELL'INCARICO

MATERIA DISCIPLINATA	Assunzioni e buste paga
DURATA DEL TRATTAMENTO	• I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
DESCRIZIONE DEI TRATTAMENTI	Intrattiene per conto dell'azienda le relazioni con i lavoratori (dipendenti, soci, amministratori, collaboratori), cura l'iscrizione dei dipendenti agli Istituti previdenziali di competenza, gestisce la redazione e stipula dei rapporti di lavoro aziendali di carattere obbligatorio, tipico ed atipico: assunzioni, cessazioni, trasferimenti, contratti, convenzioni, appalti, ecc. Elabora paghe e contributi. Assolve agli adempimenti previdenziali e assicurativi. Offre consulenza tecnica in sede di contenzioso. Offre consulenza tecnica in materia di lavoro.
FINALITÀ	• Contratto di assunzione • Elaborazione buste paga
TIPO DI DATI PERSONALI	• Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) • Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro) • Personali
CATEGORIE DI INTERESSATI	• Dipendenti
DESTINAZIONE DEI DATI ALLA CONCLUSIONE DEL CONTRATTO	Cancellazione dei dati

Lettera di incarico

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME PARTNER

Il soggetto nominato avrà il compito di trattare i dati personali riferiti alle seguenti attività di trattamento, in cui è coinvolto come partner:

Sede Operativa
Registro Dipendenti

- Gestione del Rapporto di Lavoro
  - Conservazione
  - Consultazione
  - Elaborazione

COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

in applicazione del considerando art. 28 del Regolamento UE 2016/679 e della normativa nazionale in vigore

PRINCIPI GENERALI DA OSSERVARE

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale e per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
  - secondo il principio di liceità, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
  - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- i dati devono essere raccolti solo per scopi:
  - determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
  - espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
  - legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
  - compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;
- i dati devono, inoltre, essere:
  - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
  - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
  - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
  - non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
  - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare, come previsto dall'art.28 e dall'art.30 comma 2 del Regolamento GDPR:

a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
b) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
   - il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
   - le categorie dei trattamenti effettuati;
   - se del caso, i trasferimenti di dati personali verso Paesi terzi;
   - descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;
c) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;
e) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
f) adempiere agli obblighi di sicurezza, quali:
   - adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
   - assicurarsi la capacità di ripristinare tempestivamente la disponibilità e

l'accesso ai dati in caso di incidente fisico o tecnico;
- testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
h) su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
i) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;
j) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
k) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;
l) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.
m) dare riscontro preventivo dell'eventuale trasferimento dei dati verso paesi extra UE, la cui normativa non è equiparabile a quella Europea, applicando preventivamente garanzie adeguate a tale trasferimento;
n) ricorrere ad un altro responsabile, per gestire attività di trattamento specifiche, solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento (articolo 28 comma 2 Regolamento GDPR).

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.
L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.
Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico
Il Responsabile del trattamento
(AMJ s.r.l.)

_____
(firma)

Il titolare del trattamento
(Michele De Palo)

_____
(firma)

Lettera di incarico

Torino, 26/03/2019

Oggetto: Lettera di nomina al Responsabile esterno del trattamento dati

Il sottoscritto De Palo Michele, c.f. DPLMHL84P11F335R, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e della normativa nazionale in vigore,

NOMINA

Wea s.r.l., p.iva 07103660010 Responsabile esterno del trattamento dei dati per la sede Operativa, Via Lombardi n°8, 10028 Trofarello (TO), dalla data del 26/03/2019, con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate.
In qualità di Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonchè le istruzioni impartite dal Titolare.

REQUISITI DELL'INCARICO

MATERIA DISCIPLINATA	Sicurezza sul lavoro
DURATA DEL TRATTAMENTO	• I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
DESCRIZIONE DEI TRATTAMENTI	Consulenza in materia di sicurezza sul lavoro per predisposizione Documento di Valutazione dei Rischi e per rilascio degli attestati riguardanti i corsi di formazione obbligatoria per la categoria aziendale.
FINALITÀ	• Predisposizione documentazione sicurezza sul lavoro e rilascio attestati corsi di formazione.
TIPO DI DATI PERSONALI	• Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) • Nominativo, indirizzo o altri elementi di identificazione personale (nome, cognome, età, sesso, luogo e data di nascita, indirizzo privato, indirizzo di lavoro)
CATEGORIE DI INTERESSATI	• Dipendenti
DESTINAZIONE DEI DATI ALLA CONCLUSIONE DEL CONTRATTO	Cancellazione dei dati

Lettera di incarico

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME PARTNER

Il soggetto nominato avrà il compito di trattare i dati personali riferiti alle seguenti attività di trattamento, in cui è coinvolto come partner:

Sede Operativa
Registro Dipendenti

- Gestione del Rapporto di Lavoro
  - Conservazione
  - Consultazione
  - Elaborazione

COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

in applicazione del considerando art. 28 del Regolamento UE 2016/679 e della normativa nazionale in vigore

PRINCIPI GENERALI DA OSSERVARE

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale e per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
  - secondo il principio di liceità, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
  - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- i dati devono essere raccolti solo per scopi:
  - determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
  - espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
  - legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
  - compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;
- i dati devono, inoltre, essere:
  - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
  - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
  - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
  - non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
  - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare, come previsto dall'art.28 e dall'art.30 comma 2 del Regolamento GDPR:

a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
b) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
   - il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
   - le categorie dei trattamenti effettuati;
   - se del caso, i trasferimenti di dati personali verso Paesi terzi;
   - descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;
c) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;
e) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
f) adempiere agli obblighi di sicurezza, quali:
   - adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
   - assicurarsi la capacità di ripristinare tempestivamente la disponibilità e

l'accesso ai dati in caso di incidente fisico o tecnico;
- testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
h) su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
i) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;
j) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
k) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;
l) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.
m) dare riscontro preventivo dell'eventuale trasferimento dei dati verso paesi extra UE, la cui normativa non è equiparabile a quella Europea, applicando preventivamente garanzie adeguate a tale trasferimento;
n) ricorrere ad un altro responsabile, per gestire attività di trattamento specifiche, solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento (articolo 28 comma 2 Regolamento GDPR).

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.
L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.
Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico
Il Responsabile del trattamento
(Wea s.r.l.)

_____
(firma)

Il titolare del trattamento
(Michele De Palo)

_____
(firma)

Lettera di incarico

Torino, 26/03/2019

Oggetto: Lettera di nomina al Responsabile esterno del trattamento dati

Il sottoscritto De Palo Michele, c.f. DPLMHL84P11F335R, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e della normativa nazionale in vigore,

NOMINA

Danea Soft s.r.l., p.iva 03365450281 Responsabile esterno del trattamento dei dati per la sede Operativa, Via Lombardi n°8, 10028 Trofarello (TO), dalla data del 26/03/2019, con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate.
In qualità di Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonchè le istruzioni impartite dal Titolare.

REQUISITI DELL'INCARICO

MATERIA DISCIPLINATA	Fornitura e assistenza del software gestionale
DURATA DEL TRATTAMENTO	• La durata dei trattamenti sarà limitata al tempo necessario a dare esecuzione al contratto, salvo quanto necessario per precostituire prova dell'esatto adempimento (fino allo spirare dei termini di prescrizione dei diritti obbligatori nascenti dalle prestazioni oggetto del contratto) e per norma di legge.
DESCRIZIONE DEI TRATTAMENTI	Nello svolgimento delle attività di Fornitura e assistenza del software gestionale il Responsabile può accedere ai dati di contatto dei clienti e dei fornitori. Può procedere alla copia degli archivi del Titolare nei propri strumenti informatici al fine di effettuare tutte le verifiche opportune senza mettere in pericolo la disponibilità dei dati originali trattati dal Titolare (es. perdita, distruzione in conseguenza all'attività di verifica).Resta comunque inteso che tali copie devono essere immediatamente cancellate al termine dell'attività di verifica e non possono in nessun caso essere conservate.
FINALITÀ	• Ripristino e manutenzione software gestionale
TIPO DI DATI PERSONALI	• Dati di contatto di clienti e fornitori
CATEGORIE DI INTERESSATI	• Clienti • Fornitori • Potenziali clienti
DESTINAZIONE DEI DATI ALLA CONCLUSIONE DEL CONTRATTO	Cancellazione dei dati

Lettera di incarico

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME PARTNER

Il soggetto nominato avrà il compito di trattare i dati personali riferiti alle seguenti attività di trattamento, in cui è coinvolto come partner:

Sede Operativa
Registro Fatturazione

- Gestione dei Fornitori
  - Conservazione

Sede Operativa
Registro Fatturazione

- Gestione dei Clienti
  - Conservazione

COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

in applicazione del considerando art. 28 del Regolamento UE 2016/679 e della normativa nazionale in vigore

PRINCIPI GENERALI DA OSSERVARE

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale e per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
  - secondo il principio di liceità, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
  - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- i dati devono essere raccolti solo per scopi:
  - determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
  - espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
  - legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;
  - compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;
- i dati devono, inoltre, essere:
  - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
  - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
  - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
  - non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
  - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed

i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare, come previsto dall'art.28 e dall'art.30 comma 2 del Regolamento GDPR:

a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
b) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
   - il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
   - le categorie dei trattamenti effettuati;
   - se del caso, i trasferimenti di dati personali verso Paesi terzi;
   - descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;
c) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;
e) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
f) adempiere agli obblighi di sicurezza, quali:
   - adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
   - definire una politica di sicurezza per assicurare su base permanente la

riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
- assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
h) su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
i) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;
j) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
k) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;
l) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.
m) dare riscontro preventivo dell'eventuale trasferimento dei dati verso paesi extra UE, la cui normativa non è equiparabile a quella Europea, applicando preventivamente garanzie adeguate a tale trasferimento;
n) ricorrere ad un altro responsabile, per gestire attività di trattamento specifiche, solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento (articolo 28 comma 2 Regolamento GDPR).

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.
L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.
Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico
Il Responsabile del trattamento
(Danea Soft s.r.l.)

_____
(firma)

Il titolare del trattamento
(Michele De Palo)

_____
(firma)

Lettera di incarico

Torino, 26/03/2019

Oggetto: Lettera di nomina al Responsabile esterno del trattamento dati

Il sottoscritto De Palo Michele, c.f. DPLMHL84P11F335R, in qualità di titolare del trattamento dei dati ai sensi del GDPR 2016/679 e della normativa nazionale in vigore,

NOMINA

Linuxon di Marengo Piercarlo, p.iva 09347810013 Responsabile esterno del trattamento dei dati per la sede Operativa, Via Lombardi n°8, 10028 Trofarello (TO), dalla data del 26/03/2019, con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate.
In qualità di Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonchè le istruzioni impartite dal Titolare.

REQUISITI DELL'INCARICO

MATERIA DISCIPLINATA	Manutenzione Hardware e Gestione Server aziendale
DURATA DEL TRATTAMENTO	• Durata corrispondente alla durata del rapporto contrattuale sottostante tra Titolare e Responsabile e potrà essere revocato in ogni momento dal Titolare, fermo restando il venir meno dello stesso al termine del rapporto contrattuale in essere.
DESCRIZIONE DEI TRATTAMENTI	Esecuzione del servizio di Assistenza Hardware e Software del Titolare, tra cui rientrano le attività di ripristino dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware. Il Responsabile, mediante credenziali di autenticazione con poteri da Amministratore, potrà avere accesso ai server, firewall e strumenti elettronici collegati alla rete interna del Titolare. Attraverso l'utilizzo delle proprie credenziali di autenticazione potrà inoltre avere accesso, previo consenso del Titolare o dei singoli incaricati del trattamento, a tutti gli archivi contenuti all'interno dei singoli pc degli incaricati, solo al fine di svolgere la corretta manutenzione della rete interna, degli apparati di sicurezza e dei software impiegati dall'azienda. Resta inteso che il Responsabile non può in nessun caso utilizzare, estrarre, modificare o altrimenti trattare i dati contenuti negli archivi informatici del Titolare ai quali ha accesso unicamente per le finalità indicate.
FINALITÀ	• Backup e recovery dati

	• Manutenzione Hardware, server, firewall. ecc.
TIPO DI DATI PERSONALI	• Dati personali e/o di contatto di clienti, fornitori e dipendenti. • Dati personali protetti dal segreto professionale
CATEGORIE DI INTERESSATI	• Clienti • Dipendenti • Fornitori
DESTINAZIONE DEI DATI ALLA CONCLUSIONE DEL CONTRATTO	Cancellazione dei dati

ELENCO ATTIVITA' DI TRATTAMENTO IN CUI È COINVOLTA COME PARTNER

Il soggetto nominato avrà il compito di trattare i dati personali riferiti alle seguenti attività di trattamento, in cui è coinvolto come partner:

Sede Operativa
Registro Dipendenti

- Gestione del Rapporto di Lavoro
  - Conservazione

Sede Operativa
Registro Fatturazione

- Gestione dei Fornitori
  - Conservazione

Sede Operativa
Registro Fatturazione

- Gestione dei Clienti
  - Conservazione

COMPITI ED ISTRUZIONI PER I RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

in applicazione del considerando art. 28 del Regolamento UE 2016/679 e della normativa nazionale in vigore

PRINCIPI GENERALI DA OSSERVARE

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale e per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
  - secondo il principio di liceità, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
  - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- i dati devono essere raccolti solo per scopi:
  - determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
  - espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
  - legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

- compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;

- i dati devono, inoltre, essere:
  - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
  - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
  - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
  - non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
  - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.
Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.
Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare, come previsto dall'art.28 e dall'art.30 comma 2 del Regolamento GDPR:

a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
b) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
   - il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
   - le categorie dei trattamenti effettuati;
   - se del caso, i trasferimenti di dati personali verso Paesi terzi;
   - descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;
c) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati;
e) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
f) adempiere agli obblighi di sicurezza, quali:

- adottare, tramite il supporto del Responsabile del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
- assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;

g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
h) su scelta del titolare del trattamento, cancellare o restituirgli tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
i) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;
j) garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
k) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;
l) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.
m) dare riscontro preventivo dell'eventuale trasferimento dei dati verso paesi extra UE, la cui normativa non è equiparabile a quella Europea, applicando preventivamente garanzie adeguate a tale trasferimento;
n) ricorrere ad un altro responsabile, per gestire attività di trattamento specifiche, solo previa autorizzazione scritta, specifica o generale, del titolare del trattamento (articolo 28 comma 2 Regolamento GDPR).

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al settore di competenza.
Resta fermo, in ogni caso, che la responsabilità penale per l'eventuale uso non corretto dei dati oggetto di tutela è a carico della singola persona cui l'uso illegittimo sia imputabile.
L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega. Esso decade automaticamente alla scadenza o alla revoca dell'incarico affidato.
Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.
Una copia del presente atto di nomina viene restituita al Titolare, debitamente firmata per accettazione.

Per accettazione dell'incarico
Il Responsabile del trattamento
(Linuxon di Marengo Piercarlo)

_____
(firma)

Il titolare del trattamento
(Michele De Palo)

_____
(firma)