

Valutazione di impatto e rischi sulla protezione dei dati

01/02/2022

GDPR 2016/679 - Linee Guida

DOPOLAVORO ATAC COTRAL

Sommario

VALUTAZIONE DI IMPATTO E RISCHI SULLA PROTEZIONE DEI DATI	3
OBBLIGO DPIA	3
CRITERI DA CONSIDERARE PER OBBLIGO DPIA.....	3
REVISIONE	4
ALGORITMO VALUTAZIONE	4
1° STEP: identificazione dei trattamenti	4
2° STEP: valutazione del rischio e individuazione criteri per DPIA	4
MATRICE DEI RISCHI	5
3 STEP: DPIA – valutazione del rischio normalizzato.....	6
RISULTATI DPIA	10
Elenco attività sottoposte a DPIA	10
Attività commerciali	10
VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE	10
VALUTAZIONE DEI RISCHI	11
Gestione dei fornitori (contratti, ordini, arrivi, fatture)	12
VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE	12
VALUTAZIONE DEI RISCHI	14
Gestione dei clienti	16
VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE	16
VALUTAZIONE DEI RISCHI	17
Gestione dei dipendenti (contratti, buste paga).....	19
VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE	19
VALUTAZIONE DEI RISCHI	20
ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI	23
PREMESSA	23
UTILIZZO DEL PERSONAL COMPUTER	23
UTILIZZO DELLA RETE	24
GESTIONE DELLE PASSWORD	24
UTILIZZO DEI SUPPORTI MAGNETICI	25

UTILIZZO DI PC PORTATILI	25
USO DELLA POSTA ELETTRONICA.....	25
USO DELLA RETE INTERNET E DEI RELATIVI SERVIZI.....	26
OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI	26
NON OSSERVANZA DELLA NORMATIVA AZIENDALE	26
AGGIORNAMENTO E REVISIONE	26
ISTRUZIONE OPERATIVA DATA BREACH.....	27
ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO.....	28
PREMESSA.....	28
DEFINIZIONI	28
ADEMPIMENTI.....	29
MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI.....	29
ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI	30
Gestione strumenti elettronici (pc fissi e portatili).....	30
Gestione username e password.....	31
Installazione di hardware e software	32
Gestione posta elettronica aziendale.....	33
Gestione del salvataggio dei dati	33
Gestione dei supporti rimovibili.....	34
Gestione protezione dai virus informatici	34
ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"	34
distruzione delle copie cartacee	35
Misure di sicurezza.....	35
Prescrizioni per gli incaricati.....	35
ADDETTI ALLA MANUTENZIONE	36
OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PROTEZIONE DATI PERSONALI.....	38
NON OSSERVANZA DELLA NORMATIVA AZIENDALE.....	38
AGGIORNAMENTO E REVISIONE	38
INFORMATIVA LAVORATORI DIPENDENTI	38
BASE GIURIDICA	38
CATEGORIE DI DESTINATARI	38
DIRITTI DELL'INTERESSATO	39
PERIODO DI CONSERVAZIONE.....	39
INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI	40
BASE GIURIDICA	40
PERIODO DI CONSERVAZIONE.....	40
DIRITTI DELL'INTERESSATO	40

Valutazione di impatto e rischi sulla protezione dei dati

GDPR 2016/679 - LINEE GUIDA

VALUTAZIONE DI IMPATTO E RISCHI 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:

$$LR = P \times C$$

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:

P r o b a b i l i t à	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	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

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 prevedono 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:

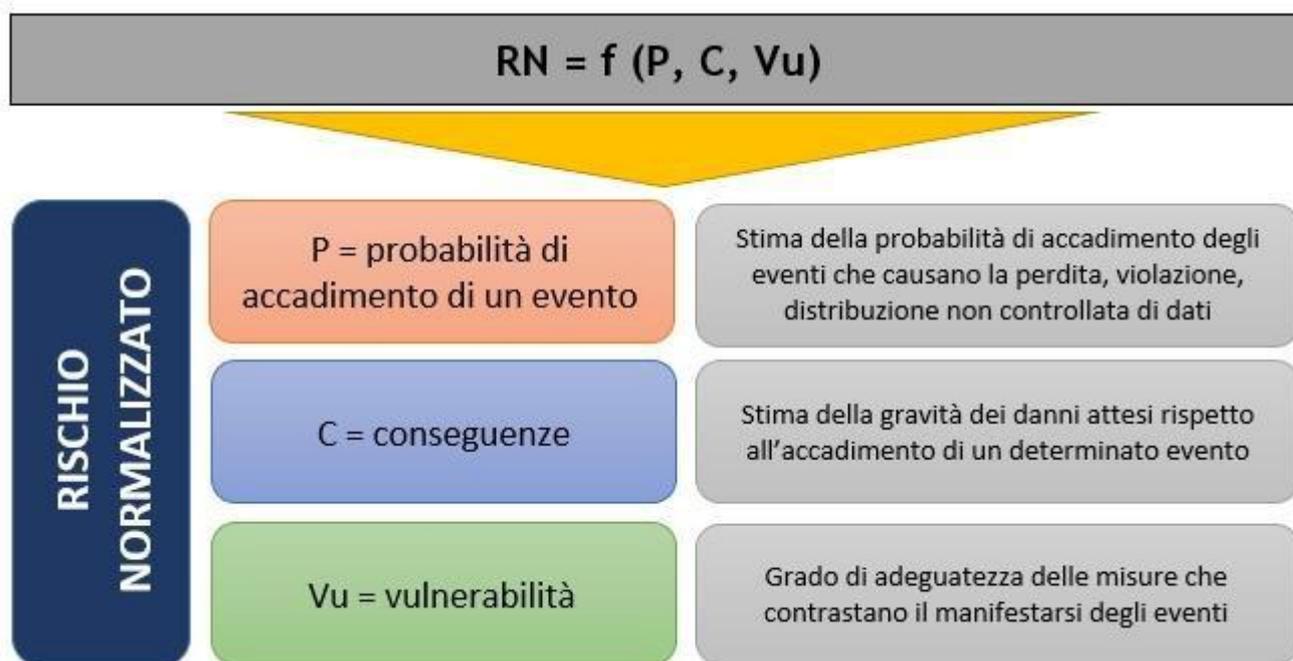
$$RN = f(P, C, Vu)$$

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 R_i 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:

P R O B A B I L I T À	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	$(1 \leq Ri \leq 2)$
Basso	$(3 \leq Ri \leq 4)$
Rilevante	$(6 \leq Ri \leq 9)$
Alto	$(12 \leq Ri \leq 16)$

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)	<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • 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.)	<ul style="list-style-type: none"> • 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.)	<ul style="list-style-type: none"> • 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.

	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
Vu	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	
$RN = Ri \times Vu$	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

- Attività commerciali (pulizia, sanificazione, derattizzazione, disinfestazione, portierato, ecc...)
- Gestione dei fornitori (contratti, ordini, arrivi, fatture)
- Gestione dei clienti
- Gestione dei dipendenti

Attività commerciali

Attività dirette alla produzione di beni o di servizi (pulizia, sanificazione, derattizzazione, disinfestazione, ecc...)

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

Sono utilizzati software antivirus e anti intrusione.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Viene eseguita opportuna manutenzione.	<ul style="list-style-type: none"> • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**

Gestione dei fornitori (contratti, ordini, arrivi, fatture)

Gestore dei contratti di fornitura

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
E' applicata una gestione della password degli utenti.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate

E' eseguita la DPIA	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti.	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Sono definiti i ruoli e le responsabilità.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate
Sono utilizzati software antivirus e anti intrusione.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Viene effettuata la registrazione ed il controllo degli accessi.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate

	elettronica, ecc.)	
Viene eseguita opportuna manutenzione.	<ul style="list-style-type: none"> • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Limitate	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Marginali	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,25	Molto basso
PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata 		

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**

Gestione dei clienti- soci

Gestione della domanda, degli ordini e delle spedizioni della merce al cliente

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
E' eseguita la DPIA.	<ul style="list-style-type: none"> Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
L'impianto elettrico è certificato ed a norma.	<ul style="list-style-type: none"> Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) Agenti fisici (incendio, allagamento, attacchi esterni) 	Adeguate
Sono definiti i ruoli e le responsabilità.	<ul style="list-style-type: none"> Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) Agenti fisici (incendio, allagamento, attacchi esterni) Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate
Sono utilizzati software antivirus e anti intrusione.	<ul style="list-style-type: none"> Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) Compromissione informazioni 	Adeguate

	(intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
Viene eseguita opportuna manutenzione.	<ul style="list-style-type: none"> • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate
Viene eseguita una regolare formazione del personale.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN

Molto basso	0,25	Molto basso
-------------	------	-------------

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		

<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio Molto basso

Gestione dei dipendenti (contratti, buste paga)

Gestore dei contratti di lavoro, buste paga, documenti anagrafici

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
E' applicata una gestione della password degli utenti.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
E' eseguita la DPIA.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate

Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti.	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Sono definiti i ruoli e le responsabilità.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) 	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate
Sono utilizzati software antivirus e anti intrusione.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Viene effettuata la registrazione ed il controllo degli accessi.	<ul style="list-style-type: none"> • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) 	Adeguate
Viene eseguita opportuna manutenzione.	<ul style="list-style-type: none"> • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Limitate	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Marginali	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
<ul style="list-style-type: none"> • Perdita • Distruzione non autorizzata • Modifica non autorizzata 		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**

ISTRUZIONI OPERATIVE UTILIZZO SISTEMI INFORMATICI

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. WALCOR 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.

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 EUROMAC 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.

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

GESTIONE DELLE PASSWORD

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal *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*.

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.

UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli dal *Responsabile dei sistemi informatici aziendali* 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.

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 WALCOR 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, ...).

È obbligatorio controllare i file attachments 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. 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.

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).

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.

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.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

ISTRUZIONE OPERATIVA DATA BREACH

L'art. 33 del **Regolamento Europeo 679/2016 (GDPR)** 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.

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:

- d. violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- e. violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- f. 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:

10. **Rischio assente:** la notifica al Garante non è obbligatoria.
11. **Rischio presente:** è necessaria la notifica al Garante.
12. **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.

ISTRUZIONI OPERATIVE INCARICATI DEL TRATTAMENTO

PREMESSA

Il presente documento contiene le istruzioni operative per gli Incaricati del trattamento dei dati personali dell'Azienda conformemente al Regolamento (Ue) 2016/679 (GDPR). 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 diversa finalità strettamente professionali, è espressamente vietato. Di seguito vengono espone 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.

DEFINIZIONI

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR), 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.

ADEMPIMENTI

Ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR), 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 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.

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.

- Rilevazione presenze

Ove possibile, si raccomanda di dotare le sedi dell'Azienda di un servizio di rilevazione delle presenze e di un servizio di reception / sorveglianza. In questo caso, ogni Incaricato è tenuto ad utilizzare sempre i sistemi di rilevazione presenze disponibili, allo scopo di segnalare la propria presenza e legittimare le attività in corso di svolgimento.

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:

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.

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:

- Almeno ogni 3 mesi è obbligatorio cambiare la password;
- 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.

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.

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 della Associazione 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;

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 involontarie.

- Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti...). L'Incaricato deve verificare che i supporti informatici utilizzati per il backup, che normalmente sono dischi magnetici esterni, CD, DVD oppure flash disks (chiavette) siano funzionali e non corrotti.

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.

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.

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.

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 verificano 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;

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.

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 contenenti 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.

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

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.

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.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione con frequenza annuale.

INFORMATIVA LAVORATORI DIPENDENTI

La scrivente che, per l'instaurazione e la gestione del rapporto di lavoro in corso, è titolare di dati Suoi e dei Suoi familiari qualificati come dati personali ai sensi del Regolamento 2016/679.

BASE GIURIDICA

- g. 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 per l'azienda di dare esecuzione al contratto o di svolgere correttamente tutti gli adempimenti, quali quelli di natura retributiva, contributiva, fiscale e assicurativa, connessi al rapporto di lavoro (2).

CATEGORIE DI DESTINATARI

Nella gestione dei suoi dati, inoltre, possono venire a conoscenza degli stessi le seguenti categorie di persone autorizzate e/o responsabili interni ed esterni individuati per iscritto ed ai quali sono state fornite specifiche istruzioni scritte circa il trattamento dei dati:

Sig.ra

- h. In relazione al rapporto di lavoro, l'azienda potrà trattare dati che la legge definisce "particolari" in quanto idonei a rilevare ad esempio:
- 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);
 - 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 (4).

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** nei limiti ed alle condizioni previste dall'art. 12 del Regolamento stesso.

PERIODO DI CONSERVAZIONE

- i. Tutti i dati predetti e gli altri costituenti il Suo stato di servizio verranno conservati anche dopo la cessazione del rapporto di lavoro per l'espletamento di tutti gli eventuali adempimenti connessi o derivanti dalla conclusione del rapporto di lavoro stesso (5).
- j. Titolare del trattamento dei Suoi dati personali è WALCOR SRL.

INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI

I dati personali dell'utente sono utilizzati da che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679.

BASE GIURIDICA

- k. 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.

PERIODO DI CONSERVAZIONE

- l. I dati obbligatori ai fini contrattuali e contabili sono conservati per il tempo necessario allo svolgimento del rapporto commerciale e contabile.
- I dati di chi non acquista o usufruisce di prodotti/servizi, pur avendo avuto un precedente contatto con dei rappresentanti dell'azienda, saranno immediatamente cancellati o trattati in forma anonima, ove la loro conservazione non risulti altrimenti giustificata, salvo che sia stato acquisito validamente il consenso informato degli interessati relativo ad una successiva attività di promozione commerciale o ricerca di mercato.

Il periodo di conservazione dei dati è: limitato alla durata del rapporto professionale e non oltre 10 anni dall'acquisizione.

DIRITTI DELL'INTERESSATO

- m. Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale, 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);
 - 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;
 - 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.

- n. Titolare del trattamento dei Suoi dati personali è

INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI

I dati personali dell'utente sono utilizzati da, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dal Regolamento GDPR 2016/679.

BASE GIURIDICA

- o. 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.

PERIODO DI CONSERVAZIONE

- p. I dati obbligatori ai fini contrattuali e contabili sono conservati per il tempo necessario allo svolgimento del rapporto commerciale e contabile.

I dati di chi non acquista o usufruisce di prodotti/servizi, pur avendo avuto un precedente contatto con dei rappresentanti dell'azienda, saranno immediatamente cancellati o trattati in forma anonima, ove la loro conservazione non risulti altrimenti giustificata, salvo che sia stato acquisito validamente il consenso informato degli interessati relativo ad una successiva attività di promozione commerciale o ricerca di mercato.

Il periodo di conservazione dei dati è: limitato alla durata del rapporto professionale e non oltre 10 anni dall'acquisizione.

DIRITTI DELL'INTERESSATO

- q. Ai sensi del Regolamento europeo 679/2016 (GDPR) e della normativa nazionale, 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);
- 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;
- 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.

- r. Titolare del trattamento dei Suoi dati personali è DOPOLAVORO ATAC COTRAL.....
- s. DPO DOTT. PAOLO FRANCO