



PANELETTRIC SRL
Via di Nettuno 35
00049 VELLETRI (RM)
Cod.Fiscale/P.IVA: 02517420598

CODICE DI CONDOTTA

Redatto il 24/09/2018

secondo quanto disposto da:
Regolamento Europeo 679/2016 (GDPR)
e dalle successive integrazioni e indicazioni del Garante Italiano per la Privacy

INDICE

1. REVISIONI.....	3
2. SCOPO	4
3. CAMPO DI APPLICAZIONE.....	5
4. RIFERIMENTI NORMATIVI.....	6
5. REGOLE GENERALI	7
5.1 ACCESSO AI LOCALI DELLA SEDE DEI DIPENDENTI E DEI COLLABORATORI	7
5.2 ACCESSO AI LOCALI DELLA SEDE DI Clienti, Visitatori e Fornitori	7
5.3 ACCESSO ALLA SALA RIUNIONI E CORSI	7
5.4 ACCETTAZIONE MERCE	7
5.5 ACCETTAZIONE APPARECCHIATURE DA RIPARARE	7
5.6 ORARIO DI LAVORO	7
5.7 PROVVEDIMENTI DISCIPLINARI	7
5.8 DIVIETO DI FUMO	7
6. UTILIZZO DELLE ATTREZZATURE E DEGLI IMPIANTI	8
6.1 SCRIVANIA E POSTI DI LAVORO	8
6.2 USO DEI PERSONAL COMPUTER E DELLE STAMPANTI	8
6.3 SISTEMI ANTIVIRUS	8
6.4 USO DEL TELEFONO	8
6.5 PRESCRIZIONI INTERNE SULLA SICUREZZA DEI DATI E DEI SISTEMI	8
6.6 UTILIZZO DI COLLEGAMENTI INTERNET	9
6.7 ACCESSO ALLA POSTA ELETTRONICA	9
6.8 UTILIZZO DELLE AUTO E DEI MEZZI AZIENDALI	10
6.9 UTILIZZO DEI DUPLICATORI DI CD-ROM	10
7. TRASFERTE E RIMBORSI	11
7.1 TRASFERTE DI LAVORO	11
8. FERIE E PERMESSI	12
9. PRELIEVO DI ATTREZZATURE	13
9.1 PRELIEVO DI DOCUMENTI	13
9.2 COMPUTER, STAMPANTI E SCANNER	13
10. ALLEGATI	14
11. DIFFUSIONE E COMUNICAZIONE	14

1. REVISIONI
Indice delle revisioni

Rev.	Data	Descrizione	Redatto	Verificato	Approvato

2. SCOPO

Il presente Codice di Condotta disciplina il trattamento dei dati personali contenuti nelle banche dati organizzate, gestite od utilizzate dall'azienda PANELETTRIC SRL, in relazione allo svolgimento delle proprie finalità istituzionali, in attuazione del **Regolamento Europeo 679/2016 (GDPR)**.

Per finalità istituzionali, ai fini del presente Codice di Condotta, si intendono le funzioni previste dalla legge, dallo Statuto, dai regolamenti, le funzioni svolte per mezzo di convenzioni, accordi, intese e mediante gli strumenti di programmazione negoziata previsti dalla legislazione vigente e le funzioni collegate all'accesso ed all'erogazione dei servizi resi ai Clienti

Ai fini del presente Codice di Condotta, per le definizioni di banca dati, di trattamento, di titolare, di responsabile, di incaricato, di interessato, di comunicazione, di diffusione, di dato anonimo, di blocco e di Garante si fa riferimento a quanto previsto dal **Regolamento Europeo 679/2016 (GDPR)**.

Il presente Codice di Condotta si redige allo scopo di formalizzare e testimoniare la responsabilizzazione del titolare del trattamento dei dati personali sulle problematiche della tutela e della riservatezza dei dati e ciò a prescindere su l'azienda ed è predisposto per eventuale integrazione di personale. Il Codice di Condotta dell'azienda PANELETTRIC SRL disciplina quindi i comportamenti correlati al trattamento dei dati personali compreso il titolare del trattamento anche se trattasi di Ditta Individuale.

Il presente Codice di Condotta deve servire per migliorare l'efficienza interna e i servizi forniti ai Clienti.

Viene adottato un Codice di Condotta standard, revisionato e adattato alle specifiche e particolari esigenze, che possa essere applicabile anche in caso di future implementazione del personale.

3. CAMPO DI APPLICAZIONE

Il "CODICE DI CONDOTTA" definisce regole e gli standard di comportamento nei confronti di tutti coloro che a qualsiasi titolo operano nei nostri locali, dei collaboratori esterni e dei fornitori in genere.

Il "CODICE DI CONDOTTA" riguarda tutti coloro che operano all'interno della azienda PANELETTRIC SRL ed in particolare:

- Il personale dipendente

- I collaboratori esterni

- Coloro che per motivi vari si trovano anche temporaneamente ad operare all'interno dei nostri locali.

Il "CODICE DI CONDOTTA" deve essere conosciuto ed applicato da tutte le componenti della nostra attività..

A cura del Titolare, possono essere periodicamente attivati controlli, anche a campione, al fine di garantire la sicurezza delle banche-dati, e l'attendibilità dei dati inseriti e il rispetto delle norme e disposizioni previste dal DPSS e dal presente regolamento.

4. RIFERIMENTI NORMATIVI

Contratto nazionale di Lavoro

Decreto legislativo 19 settembre 1994 n. 626 sulla "sicurezza e salute dei lavoratori durante il lavoro"

Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"

Le linee guida del Garante per posta elettronica e internet pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007

Legge antifumo

Garante per la Protezione dei Dati Personali con Provvedimento n. 456 del 30 luglio 2015

Regolamento Europeo 679/2016 (GDPR)

Linee-guida del Garante sulla valutazione d'impatto della protezione dati (04/10/2017)

Decreto Legislativo del 21 Agosto 2018 n. 101

5. REGOLE GENERALI

5.1 ACCESSO AI LOCALI DELLA SEDE

I dipendenti, i fornitori e i consulenti possono accedere ai locali degli uffici durante l'orario programmato con eccezione per le funzioni esplicitamente autorizzate dal Titolare.

5.2 ACCESSO AI LOCALI DELLA SEDE DEI Clienti

I Clienti potranno accedere ai locali della sede durante l'orario programmato sia per riunioni o presentazioni che per prenotare appuntamenti o chiedere informazioni. **I Clienti non possono avere accesso in punti in cui è possibile avere visuale degli schermi dei computer.**

5.3 ACCESSO ALLE SALE PER RIUNIONI, INCONTRI E CORSI

Le persone che devono partecipare a riunioni, incontri e corsi tenuti presso gli uffici, potranno accedere direttamente seguendo le indicazioni del personale addetto.

5.4 ACCETTAZIONE MERCE

I trasportatori e i fornitori che consegnano merce hanno la possibilità di farlo esclusivamente durante l'orario di ufficio e avranno accesso solo all'ingresso. Per lo scarico diretto di merci in un locale interno dovranno essere accompagnati dal personale addetto.

5.5 RITIRO DOCUMENTI

I Clienti (o i loro delegati) che devono ritirare documenti possono presentarsi in Segreteria negli orari affissi.

5.6 ORARIO DI LAVORO E DI LEZIONE

L'orario di lavoro è deve essere rispettato da tutto il personale dipendente secondo le indicazioni e le turnazioni previste e programmate..

5.7 PROVVEDIMENTI DISCIPLINARI

Incorre nei provvedimenti previsti dall'art.24 del Contratto Nazionale di Lavoro (ammonizione scritta, multa o sospensione) il personale dipendente che:

Non si presenta al lavoro o abbandoni il proprio posto di lavoro senza giustificato motivo oppure non giustifichi l'assenza entro il giorno successivo a quello dell'inizio dell'assenza stessa, salvo il caso di impedimento giustificato.

Senza giustificato motivo ritardi l'inizio del lavoro o lo sospenda o ne anticipi la cessazione.

5.8 DIVIETO DI FUMO

Nel rispetto della salute di tutti è **VIETATO FUMARE** all'interno dell'azienda. Il divieto è esteso ai Clienti, ai Fornitori e a chiunque sia all'interno dell'azienda. Appositi cartelli segnalano il divieto e informano della possibilità che un responsabile designato possa comminare una multa.

6. UTILIZZO DELLE ATTREZZATURE E DEGLI IMPIANTI

6.1 SCRIVANIA E POSTI DI LAVORO

Ognuno è tenuto a conservare con la massima cura tutto il materiale che gli è stato affidato. Ogni incaricato deve tenere in ordine la propria scrivania e gli armadi evitando di tenere in vista bottiglie vuote, lattine, bicchieri usati, ecc.. e deve preoccuparsi di spegnere computer, stampanti, fotocopiatrici ogni qualvolta si lascia il posto di lavoro, in particolare durante l'intervallo di pranzo e la sera e comunque secondo le disposizioni ricevute dal Responsabile. Ognuno si deve preoccupare di controllare la chiusura delle finestre e, se presenti, di porte o grate di sicurezza. Se per motivi di lavoro ci si sposta dal proprio posto di lavoro ad un altro per un periodo prolungato si deve comunicare al Responsabile dove ci si trova.

6.2 USO DEI PERSONAL COMPUTER E DELLE STAMPANTI

Il personal computer a disposizione per lavorare e le stampanti debbono essere tenute in uno stato di buona efficienza.

Se si riscontrano anomalie di funzionamento si deve far intervenire prontamente l'assistenza tecnica secondo la procedura prevista dal Responsabile (moduli di segnalazione).

6.3 SISTEMI ANTIVIRUS

Su tutti i personal computer interni **deve essere installato un sistema Antivirus**, conformemente alle indicazioni dell'Amministratore di Rete. Se si riscontrano anomalie di funzionamento si deve informare immediatamente l'Amministratore di Rete o il Responsabile.

6.4 USO DEL TELEFONO

Il telefono è uno strumento di lavoro e va utilizzato esclusivamente per questo scopo. **Per nessun motivo si deve disporre il telefono in modo che non possano essere ricevute telefonate.** Si raccomanda di effettuare comunicazioni brevi e precise e di annotare le eventuali richieste sulla apposita modulistica. Le telefonate personali vanno limitate allo stretto necessario sia in numero che in durata. L'uso del telefono personale (cellulare) è consentito per sole emergenze e in casi di effettiva necessità per chiamate brevi con l'obiettivo di evitare il più possibile disagi ai Clienti o rallentamenti significativi del normale svolgimento di lavoro.

6.5 PRESCRIZIONI INTERNE SULLA SICUREZZA DEI DATI E DEI SISTEMI

Per i trattamenti di dati personali effettuato con l'ausilio di strumenti elettronici, gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- Gli Incaricati del trattamento dei dati personali sono autorizzati ad effettuare esclusivamente i trattamenti di dati personali che rientrano nell'ambito di trattamento definito per iscritto e comunicato all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati comunali che contengono i predetti dati personali.
- Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate e, pertanto, in conformità alle informazioni comunicate agli interessati.
- L'Incaricato del trattamento dei dati personali deve prestare particolare attenzione all'esattezza dei dati trattati e, se sono inesatti o incompleti, deve provvedere ad aggiornarli tempestivamente.
- Ogni Incaricato del trattamento dei dati personali è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione o perdita anche accidentale dei dati, accesso non autorizzato, trattamento non consentito o non conforme alle finalità della raccolta.
- Gli Incaricati del trattamento dei dati personali che hanno ricevuto le credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le componenti riservate delle credenziali di autenticazione (parole chiave) e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
- La componente riservata delle credenziali di autenticazione (parola chiave) non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'Incaricato del trattamento dei dati personali deve modificare la componente riservata delle credenziali di autenticazione (parola chiave) al primo utilizzo e, successivamente, almeno ogni sei mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la componente riservata delle credenziali di autenticazione (parola chiave) deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali. Per i trattamenti di dati personali effettuato senza l'ausilio di strumenti elettronici gli Incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere portati al di fuori dei locali o negli armadi individuati per la loro conservazione se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Per tutto il periodo in cui i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici sono al di fuori dei locali individuati per la loro conservazione o dagli armadi, l'incaricato del trattamento non dovrà lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri.
- Al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione.
- I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Si deve adottare ogni cautela affinché ogni persona non autorizzata, non possa venire a conoscenza del contenuto di documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici.
- Per evitare il rischio di diffusione dei dati personali trattati senza l'ausilio di strumenti elettronici, si deve limitare l'utilizzo di copie fotostatiche al minimo indispensabile.
- Particolare cautela deve essere adottata quando i documenti sono consegnati in originale a un altro incaricato debitamente autorizzato;
- Documenti contenenti dati personali sensibili o dati che, per una qualunque ragione siano stati indicati come meritevoli di particolare attenzione, devono essere custoditi con molta cura.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- Quando i documenti devono essere trasportati essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti.
- L'incaricato del trattamento deve inoltre evitare che un soggetto terzo non autorizzato al trattamento possa esaminare, anche solo la copertina del documento in questione.
- E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione.
- Si raccomanda vivamente non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente. Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

6.6 UTILIZZO DI COLLEGAMENTI INTERNET

Per la tipologia di lavoro e per i vantaggi che derivano dall'utilizzo di INTERNET, sono messe a disposizione di tutto il personale le migliori tecnologie oggi disponibili. **Sono vietati comunque i collegamenti ad INTERNET per usi non strettamente collegati al lavoro da svolgere, e debbono essere evitate tutte le attività non strettamente necessarie (come ad esempio l'utilizzo di siti internet per ascoltare radio, download di film, canzoni, ecc...).** Non è ammesso l'utilizzo di collegamenti per servizi o scopi personali, quali Servizi di Borsa, Prenotazione viaggi, ecc.. Si informa il personale che per effetto di copie di back up, della gestione tecnica della rete o di files di log sono conservate informazioni sulla navigazione degli utenti in forma centralizzata. Tale registrazione è obbligatoria e può essere esibita all'autorità giudiziaria in caso di richiesta di quest'ultima.

6.7 ACCESSO ALLA POSTA ELETTRONICA

Per fronteggiare le recenti minacce di software indesiderato in grado di modificare i dati aziendali (definito in vari modi tra i quali virus, ramsonware, cryptovirus, encryptor) stante le avvertenze della case produttrici di antivirus, antispyware e altri sistemi di sicurezza e prevenzione, e stabilito che l'origine più frequente delle infezioni virali di questo tipo di software avviene attraverso la posta elettronica, si diramano le seguenti direttive:

1. Chiunque adoperi software di posta elettronica (client) o consulti la posta elettronica attraverso un qualsiasi browser (webmail) deve prestare particolare attenzione al mittente ed all'oggetto ed astenersi anche solo dall'aprire il messaggio, se possibile, in caso di mittenti sconosciuti, di oggetto non coerente o palesemente erraneo, non conforme o vuoto.
2. Nei messaggi di posta elettronica prestare particolare attenzione ad eventuali collegamenti (link) contenuti nel testo del messaggio ed evitare di seguire il li collegamento (clic sul link) se puntano ad indirizzi stranieri, a file di tipo eseguibile (.EXE) o file di programma (.JAR, .MSI, ecc)
3. Nei messaggi di posta elettronica prestare particolare attenzione ai file allegati ed evitare di scaricarli (download) se sospetti o sconosciuti.

4. Nel caso in cui sul proprio pc compaiono messaggi di richiesta di denaro (in italiano o in altra lingua) e appare impossibile aprire i propri file, è necessario staccare immediatamente il cavo di rete del pc e richiedere immediatamente l'intervento del proprio amministratore di rete

Tali disposizioni si applicano anche se l'utente consulta la posta elettronica personale: il Garante per la Protezione dei Dati Personali con Provvedimento n. 456 del 30 luglio 2015 ha stabilito che il datore di lavoro, pur non avendo il diritto di accedere ai contenuti specifici, ha il diritto di verificare l'utilizzo della posta elettronica aziendale al fine di prevenire infezioni virali e garantire la massima sicurezza possibile estendendo tale diritto a tutte le attività svolte dal dipendente, con le attrezzature aziendali, ivi compresa la consultazione della posta elettronica personale se effettuata nelle ore di ufficio anche con mezzi propri (mobile, tablet, ecc) se commessi tramite la rete aziendale.

6.8 UTILIZZO DELLE AUTO E DEI MEZZI AZIENDALI

Le auto e i mezzi aziendali vanno usate con cura e con la massima attenzione nel rispetto del codice della strada. Ognuno è responsabile per il modo in cui vengono utilizzate le auto, ed **eventuali sanzioni o contravvenzioni sono a carico del dipendente** in base al concetto di responsabilità personale, anche durante le trasferte di lavoro. I dipendenti che hanno avuto assegnata un mezzo o che ne siano responsabili, debbono preoccuparsi di **effettuare tutte le normali manutenzioni necessarie** a mantenere efficiente il mezzo.

6.9 UTILIZZO DEI DUPLICATORI DI CD/DVD (Masterizzatori)

I duplicatori di CD/DVD debbono essere utilizzati nel rispetto delle leggi sul Copyright.

7. TRASFERTE E RIMBORSI

7.1 TRASFERTE DI LAVORO

Il personale che deve effettuare trasferite di lavoro è obbligato a darne comunicazione anticipata al Responsabile o essere da questi esplicitamente autorizzato, indicando anche eventuali successivi spostamenti, in modo che, per quanto possibile, ognuno durante il normale orario di lavoro sia reperibile in qualsiasi momento.

8. FERIE E PERMESSI

I permessi e le ferie debbono essere richiesti per iscritto tramite apposito modulo. Incorre nei provvedimenti previsti dall'art. 24 del Contratto Nazionale di Lavoro (ammonizione scritta, multa o sospensione) il personale dipendente che senza giustificato motivo si assenti dal lavoro o lo sospenda o ne anticipi la cessazione senza che gli sia stato autorizzato con un permesso o un periodo di ferie.

9. PRELIEVO DI ATTREZZATURE

9.1 PRELIEVO DI DOCUMENTI

Di regola i documenti aziendali non si possono prendere e portare fuori della sede con la sola unica eccezione dei trasferimenti presso le autorità giudiziarie previa autorizzazione del Responsabile. In tutti i casi in cui si renda necessario, comunque, possono essere prelevati esclusivamente per gli scopi autorizzati e per il tempo strettamente necessario.

9.2 COMPUTER, STAMPANTI E SCANNER

L'utilizzo di computer (soprattutto dispositivi portatili), stampanti e scanner fuori dalla sede debbono essere autorizzati e deve esserne fatta richiesta scritta direttamente al Responsabile indicando:

Chi ne fa richiesta

Lo scopo

La destinazione

Quando il materiale verrà prelevato dalla sede.

Quando il materiale verrà riportato in sede.

10. ALLEGATI

Nessun allegato

11. DIFFUSIONE E COMUNICAZIONE

Il presente Codice di Condotta viene posto a conoscenza di tutti i Dipendenti, i Collaboratori, gli Operatori e alle risorse in outsourcing a mezzo:

- Firma per presa visione
- Invio tramite email
- Affissione all'albo
- Pubblicazione sul sito web
- Altro:

Il Titolare
Fabrizio Belli

(revisione del 24/09/2018)



Velletri, 24/09/2018



GDPR - R.E. 679/2016 Revisione del Documento Programmatico sulla Sicurezza

Redatto in base alle disposizioni del
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
del
CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(art.34 e Allegato B, regola 19, del d.lgs. 30 giugno 2003, 196)

Aggiornato in base al

- Provvedimento del Garante del 27/11/2008, G.U. n.300 del 24/12/2008
- Provvedimento in materia di videosorveglianza del 08/04/2010 (G.U. n. 99 del 29/04/2010)
- Decreto Legge 9 febbraio 2012, n. 5 (**semplificazione**)
- Provvedimento n. 456 del 30 luglio 2015 (sicurezza della posta elettronica)
- **Regolamento Europeo 679/2016**
- Linee-guida del Garante sulla valutazione d'impatto della protezione dati (04/10/2017)

Redatto con la consulenza di



Michele Giannini
Consulente informatico
Via Palermo 59 - 04100 LATINA
P.IVA: 01677030593
master@latinaweb.it
www.latinaweb.it



Velletri, 24/09/2018

Atto di responsabilità

Il presente documento di sintesi viene redatto ai sensi del Regolamento Europeo 679/2016 al fine di manifestare l'attenzione che il titolare **Fabrizio Belli** pone al trattamento dei dati in merito a riservatezza e sicurezza.

In proposito occorre sottolineare che c'è volontà di adeguarsi, nel trattamento e sicurezza dei dati, al dettato della normativa italiana, che fa riferimento al D. Lgs. 196/2003 e succ. mod. Tale Decreto, integrato con le precisazioni ed i suggerimenti del Garante Italiano per la Privacy, fin'ora è stato il testo base per trattare a norma i dati personali, sensibili e riservati.

Nel 2016 però la Comunità Europea ha emesso un Regolamento di disciplina della Privacy (nr. 679/2016) che integra e supera, per molti aspetti, la norma nazionale italiana. Infatti viene specificata una diversa gestione dei dati, vengono individuate nuove figure - anche esterne - all'azienda, e, in sostanza, viene rivoluzionato il concetto di privacy, di metodologia e responsabilità della tenuta dei dati.

A seguito del recente D. Lgs. 101/2018 il titolare dell'Azienda, in ottemperanza a quanto richiesto dal nuovo Regolamento Europeo sulla corretta condotta (art. 40), ha quindi ritenuto di provvedere ad implementare la normativa italiana con il nuovo regolamento europeo.

Le implementazioni hanno riguardato la predisposizione di nuove strutture e attrezzature aventi caratteristiche di agilità dinamicità e flessibilità per poter recepire eventuali osservazioni o disposizioni della competente autorità con prontezza e spirito di collaborazione implementando le attività poste in essere al fine di dar completa, puntuale ed esatta applicazione sia alla normativa nazionale che a quella Europea.

Poiché la natura delle attività svolte e la dimensione aziendale non sembrano essere riconducibili a quanto disposto dagli art. 41 e 42 circa la necessità di una certificazione esterna dei trattamenti di dati il titolare del Trattamento Dati Aziendale ha ritenuto di:

- non affidare a consulenti esterni la gestione della certificazione del trattamento dati aziendale
- non avere l'obbligo della tenuta del Registro dei Trattamenti (Art 30, comma 5)

Fermo e ribadito quanto sopra esposto, al fine di dimostrare la più ampia trasparenza nella gestione dei Dati, il titolare del Trattamento dei Dati ha deciso comunque di predisporre un registro cartaceo il cui schema è allegato al presente documento e che potrà essere utilizzato in futuro.

Il tutto in un'ottica di consapevolezza e con la certezza di operare in modo corretto.

Fabrizio Belli





Velletri, 24/09/2018

Tutela della privacy (Privacy policy)

Ai sensi del Regolamento Europeo 679/2016

La privacy è un valore che **PANELETTRIC SRL** con sede in Via di Nettuno 35 - 00049 VELLETRI (RM) (titolare del trattamento dei dati personali) riconosce e rispetta. Prima di comunicarci i Suoi dati personali, legga cortesemente l'informativa relativa all'uso che ne faremo, così come richiede la normativa europea (Regolamento Europeo 679/2016) e che si riassume brevemente nei seguenti punti:

1. I Suoi dati personali (ordinari, sensibili, giudiziari inclusi foto, video, filmati) saranno conservati negli archivi informatici e/o cartacei di **PANELETTRIC SRL** e saranno trattati nei modi e nei limiti e per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti e per un tempo superiore al solo scopo storico o statistico. I predetti dati non saranno né comunicati né diffusi.
2. Le ricordiamo che il conferimento dei Suoi dati personali è facoltativo; tuttavia, in caso di un Suo rifiuto al conferimento degli stessi, **PANELETTRIC SRL** si troverà nell'impossibilità di erogare i Servizi.
3. In presenza del Suo consenso, i Suoi dati personali potranno altresì essere utilizzati per consentire ad **PANELETTRIC SRL** di inviare comunicazioni o di effettuare attività di tipo informativo circa iniziative di diversa natura.
4. Potrà esercitare i diritti previsti dalla norma (quali ad esempio: conoscere in ogni momento i Suoi dati personali e come vengono utilizzati, farli aggiornare, rettificare, cancellare, chiederne il blocco o opporsi al trattamento) rivolgendosi a: **PANELETTRIC SRL** come indicato in testata. Presso detta società è altresì depositato l'elenco aggiornato di tutti i responsabili ed incaricati del trattamento dei Suoi dati personali.

Le ricordiamo, inoltre, che la copia completa dell'Informativa è disponibile presso la nostra sede.

Fabrizio Belli





Velletri, 24/09/2018

Necessità della valutazione di impatto

Le linee guida fornite dal Garante Italiano per la Privacy (Cfr. Linee-guida del Garante sulla valutazione d'impatto della protezione dati del 04/10/2017, Allegato 1 - Esempi di quadri UE esistenti di valutazione d'impatto sulla protezione dei dati) hanno ben individuato modi e forme per una corretta valutazione d'impatto del dato da trattare.

Alla luce di tali indicazioni il titolare del Trattamento dei Dati Aziendale precisa che la tipologia dei dati trattati non genera un 'rischio elevato' o comunque 'significativo'.

I dati trattati, infatti, sono costituiti esclusivamente da:

- dati anagrafici ed identificativi
- dati inerenti alla fattispecie della propria attività
- dati contabili ed amministrativi

Tali dati sono custoditi e conservati in sistemi informatizzati protetti da password per cui è escluso un accesso casuale, non controllato o da terzi non facultati ad accedere al dato.

Si precisa che i dati sono oggetto di periodici aggiornamenti e verifica con eliminazione fisica degli stessi dal sistema informatico ogni qualvolta la fase del trattamento sia da ritenersi, alla luce delle dinamiche operative e funzionali dell'azienda, conclusa e non più strettamente necessaria allo svolgimento dell'attività per cui sono stati acquisiti.

Non sono presenti processi decisionali automatizzati per l'estrazione di dati dalle banche dati.

Il tutto nelle more che nell'ordinamento Italiano venga delineato ufficialmente un quadro di riferimento che integri le pratiche di lavoro esistenti affinché tengano conto degli elementi costitutivi di cui all'articolo 35, paragrafo 7 (vedasi ancora le linee-guida del Garante sulla valutazione d'impatto della protezione dati del 04/10/2017, Allegato 1 - Esempi di quadri UE esistenti di valutazione d'impatto sulla protezione dei dati) cosa che, invece, è già stata normata in altri Paesi dell'Unione Europea.

Fabrizio Belli



Velletri, 24/09/2018

Il Responsabile della Protezione dei Dati

Il Titolare del Trattamento Dati analizzata la situazione del trattamento Dati aziendale, la sicurezza informatica e fisica della conservazione del dato, alla luce di quanto sancito dal Regolamento Europeo 679/2018 (Trattamento dei dati personali), valuta pertanto quanto segue.

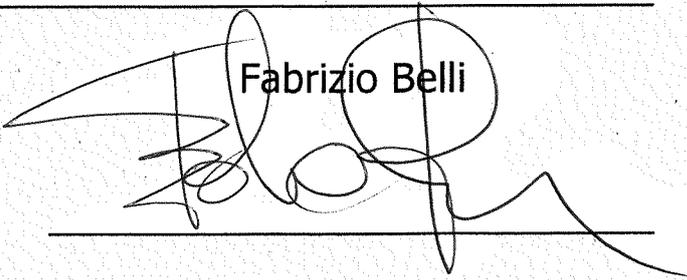
Premesso che:

- non sussistono le condizioni di cui all'art. 37, comma 1, lettere b) e c)
- le dimensioni aziendali non sono tali da consentire un incremento del personale;
- Il Titolare del Trattamento Dati ha assunto anche il ruolo di Responsabile del Trattamento dei Dati
- sono state concertate con gli altri Responsabili dell'organigramma aziendale le operazioni e le soluzioni adottate per la sicurezza e la salvaguardia dei dati trattati, nonché la corretta condotta per la raccolta e la gestione degli stessi;
- sono state valutate come non rischiose le attività di trattamento dei dati,
- in Azienda non è presente, tra i dipendenti, personale qualificato o specializzato con specifiche competenze di sicurezza informatica

non ritiene di dover procedere alla nomina di un Responsabile della Protezione dei Dati.

Si impegna altresì a rendere disponibile, all'autorità competente che ne faccia richiesta, ogni informazioni utile rilevabile dal proprio sistema informativo.

Fabrizio Belli





Velletri, 24/09/2018

Trattamento dei dati in outsourcing

Il Titolare del Trattamento Dati premesso che:

- le dimensioni aziendali non sono tali da consentire un incremento del personale e delle attrezzature;
- ha assunto anche l'incarico di Responsabile del Trattamento dei Dati;
- ha concertato con gli altri Responsabili dell'organigramma le operazioni e le soluzioni adottate per la sicurezza e la salvaguardia dei dati trattati, nonché la corretta condotta per la raccolta e la gestione degli stessi;
- ha valutato come non rischiosa l'attività di trattamento dei dati, ovvero ha valutato di non dover procedere ad una valutazione d'impatto;
- non dispone tra i suoi dipendenti di personale qualificato o specializzato con specifiche competenze di sicurezza Informatica;
- ha svolto un'indagine di mercato analizzato le garanzie di sicurezza e affidabilità di servizi cloud;
- che le società o i servizi scelti sono di grande importanza, istituzionali o di persone di fiducia già incaricate al trattamento degli stessi dati

adotta i servizi in out-sourcing descritti nell'allegato "**Dati in outsourcing**", e dichiara altresì

- di essere consapevole che i dati che trasmetterà sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
- di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
- di adottare istruzioni specifiche per il trattamento dei dati personali in out-sourcing e di integrarle nelle procedure già in essere;
- di impegnarsi a verificare periodicamente le misure di sicurezza adottate e di segnalare immediatamente ai servizi connessi le situazioni anomale o di emergenze.

Nello specifico, alla data di compilazione di questo documento, i dati riconducibili abanche dati esterne, sono elencati nel 'Registro dei Trattamenti' allegato e che di qui innanzi sarà costantemente aggiornato come disposto dall'Art. 30 del R.E. 679/2016.

Fabrizio Belli

