

**COMUNE DI PALMANOVA
PROVINCIA DI UDINE**

DECRETO

Oggetto: NOMINA DI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI (art. 4, comma 1, lettera g) del D.L.vo 196/03) GESTITI DA SOGGETTI ESTERNI.

IL SINDACO

Il sottoscritto Cressati Federico, Sindaco del Comune di Palmanova, in qualità di titolare del trattamento dei dati personali presso questo Ente;

Considerato che alcuni servizi comunali, che comportano il trattamento di dati personali, sono gestiti da soggetti esterni all'ente, quali a titolo esemplificativo il tesoriere, il concessionario pubbliche affissioni, le ditte appaltatrici di servizi;

Considerato che il Titolare deve garantire che anche tale trattamento avvenga nel rispetto delle disposizioni normative previste dal D.Lgs 196/2003 "Codice in materia di protezione dei dati personali";

nomina

quali responsabili del trattamento dei dati personali i soggetti esterni all'Ente che gestiscono un servizio comunale e trattano dati in possesso del Comune, in applicazione a quanto previsto dall'art. 4, comma 1, lettera g) del D.L.vo 196/03.

I soggetti nominati responsabili sono tenuti all'osservanza delle disposizioni previste dal D.Lgs 196/2003 "Codice in materia di protezione dei dati personali" nel trattamento dei dati personali effettuato per l'espletamento di servizi comunali.

I soggetti nominati responsabili sono tenuti inoltre all'osservanza delle disposizioni contenute nell'allegato mansionario "Regole di comportamento per una corretta gestione della privacy e della sicurezza nei luoghi di lavoro".

A tal fine devono rilasciare la dichiarazione allegata.

Palmanova, 19.03.2009

Il Sindaco
Cressati Federico

Al Comune di
Palmanova
Piazza Grande, 1
33057 PALMANOVA (UD)

Oggetto: dichiarazione osservanza disposizioni previste dal D.Lgs 196/2003 “Codice in materia di protezione dei dati personali”.

DICHIARAZIONE RESA AI SENSI DEGLI ARTT. 46 E SS DEL T.U. 445/2000

Il sottoscritto _____ nato a _____ il _____,
residente a _____ in via _____, codice
fiscale _____, in qualità di _____ della
Ditta _____ con sede a _____,
p.IVA _____

dichiara ai sensi e per gli effetti degli artt. 46 e ss del T.U. n. 445/2000,

consapevole delle sanzioni penali cui può andare incontro previste dall’art. 76 del T.U. n. 445/2000 in caso di falsità in atti e dichiarazioni mendaci, e della decadenza dei benefici conseguiti a seguito di un provvedimento adottato in base a una dichiarazione rivelatasi successivamente mendace:

- che la Ditta _____, che gestisce il seguente servizio comunale _____, come previsto con atto _____ n. _____ di data _____, nominata “responsabile del trattamento dei dati personali” con Decreto del Sindaco del 19/03/2009, accetta tale nomina, ottempera a quanto disposto dal D.Lgs 196/2003 “Codice in materia di protezione dei dati personali” nel trattamento dei dati personali effettuato per l’espletamento del servizio comunale di che trattasi, e si impegna ad osservare il mansionario “Regole di comportamento per una corretta gestione della privacy e della sicurezza nei luoghi di lavoro” pubblicato sul sito internet del Comune..

A tal fine allega inoltre copia di un proprio documento di identità personale in corso di validità.

(timbro della Ditta e firma del titolare o legale rappresentante)

_____, lì _____

REGOLE DI COMPORTAMENTO PER UNA CORRETTA GESTIONE DELLA PRIVACY E DELLA SICUREZZA NEI LUOGHI DI LAVORO

1. NON COMUNICARE A NESSUN SOGGETTO NON SPECIFICATAMENTE AUTORIZZATO I DATI PERSONALI COMUNI, SENSIBILI, GIUDIZIARI, SANITARI E/O ALTRI DATI, ELEMENTI, INFORMAZIONI DEI QUALI VENITE A CONOSCENZA NELL'ESERCIZIO DELLE VOSTRE FUNZIONI E MANSIONI PRESSO IL COMUNE DI PALMANOVA. IN CASO DI DUBBIO ACCERTARSI SEMPRE DAL TITOLARE O DAL RESPONSABILE DEL TRATTAMENTO SE IL SOGGETTO CUI DEVONO ESSERE COMUNICATI I DATI SIA O MENO AUTORIZZATO A RICEVERLI.
2. *CHIUDERE A CHIAVE CASSETTI ED UFFICI.* IL PRIMO LIVELLO DI PROTEZIONE DI QUALUNQUE SISTEMA È QUELLO FISICO. E' CERTAMENTE VERO CHE UNA PORTA CHIUSA PUÒ IN MOLTI CASI NON COSTITUIRE UNA PROTEZIONE SUFFICIENTE, MA È ANCHE VERO CHE PONE SE NON ALTRO UN PRIMO OSTACOLO, E RICHIEDE COMUNQUE UNO SFORZO VOLONTARIO NON BANALE PER LA SUA RIMOZIONE. È FIN TROPPO FACILE PER UN ESTRANEO ENTRARE IN UN UFFICIO NON CHIUSO A CHIAVE E SBIRCIARE I DOCUMENTI POSTI SU UNA SCRIVANIA O VISIBILI SU UNO SCHERMO. PERTANTO, CHIUDETE A CHIAVE IL VOSTRO UFFICIO ALLA FINE DELLA GIORNATA ED OGNI VOLTA CHE VI ASSENTATE. INOLTRE CHIUDETE I DOCUMENTI A CHIAVE NEI CASSETTI OGNI VOLTA CHE POTETE.
3. *SPEGNERE IL COMPUTER SE CI SI ASSENTA PER UN PERIODO DI TEMPO LUNGO.* LASCIARE UN COMPUTER ACCESO NON CREA PROBLEMI AL SUO FUNZIONAMENTO ED AL CONTRARIO VELOCIZZA IL SUCCESSIVO ACCESSO. TUTTAVIA, UN COMPUTER ACCESO È IN LINEA DI PRINCIPIO MAGGIORMENTE ATTACCABILE PERCHÉ RAGGIUNGIBILE TRAMITE LA RETE O DIRETTAMENTE SULLA POSTAZIONE DI LAVORO. INOLTRE, PIÙ LUNGO È IL PERIODO DI ASSENZA MAGGIORE È LA PROBABILITÀ CHE UN'INTERRUZIONE DELL'ENERGIA ELETTRICA POSSA PORTARE UN DANNO.
4. *NON LASCIARE LAVORI INCOMPIUTI SULLO SCHERMO.* CHIUDETE SEMPRE LE APPLICAZIONI CON CUI STATE LAVORANDO QUANDO VI ALLONTANATE DAL POSTO DI LAVORO PER PIÙ DI POCHI MINUTI: POTRETE RIMANERE LONTANI PIÙ DEL PREVISTO, E UN DOCUMENTO PRESENTE SULLO SCHERMO È VULNERABILE (QUASI) QUANTO UNO STAMPATO O COPIATO SU DISCHETTO.
5. *NON LASCIARE DOCUMENTI SULLA SCRIVANIA.* NON LASCIARE DOCUMENTI, LETTERE, FASCICOLI, APPUNTI SOPRA LA SCRIVANIA QUANDO VI ALLONTANATE DALLA POSTAZIONE DI LAVORO. IN PARTICOLARE NON LASCIATE SUL TAVOLO MATERIALI CHE NON SIANO INERENTI LA PRATICA CHE STATE TRATTANDO IN QUEL MOMENTO. CIÒ VALE SOPRATTUTTO NEL CASO IN CUI ABBIATE MANSIONI DI FRONT OFFICE E DI RICEZIONE DEL PUBBLICO.
6. *SALVASCHERMO.* OGNI POSTAZIONE DI LAVORO DEVE AVERE IL SALVASCHERMO ATTIVATO, CON RICHIESTA DI PASSWORD PER POTER RIPRENDERE IL CONTROLLO DELLA POSTAZIONE.
7. *PROTEGGERE ATTENTAMENTE I DATI.* BISOGNA PRESTARE PARTICOLARE ATTENZIONE AI DATI IMPORTANTI DI CUI SI È PERSONALMENTE RESPONSABILI. POICHÉ PUÒ RISULTARE DIFFICILE DISTINGUERE TRA DATI NORMALI E DATI IMPORTANTI, È BUONA NORMA TRATTARE TUTTI I DATI COME SE FOSSERO IMPORTANTI. COME MINIMO POSIZIONARLI IN UN'AREA PROTETTA DA PASSWORD E NON DARE AUTOMATICAMENTE A NESSUN ALTRO UTENTE IL PERMESSO DI LETTURA O MODIFICA. AI DATI DA CONDIVIDERE APPLICARE I PERMESSI OPPORTUNI SOLO PER IL TEMPO STRETTAMENTE NECESSARIO ALL'INTERAZIONE CON GLI ALTRI UTENTI.
8. *CONSERVARE SUPPORTI DI MEMORIA E STAMPE IN LUOGHI SICURI.* ALLA CONSERVAZIONE DEI SUPPORTI DI MEMORIA (CD, DISCHETTI) SI APPLICANO GLI STESSI CRITERI DI PROTEZIONE DEI DOCUMENTI CARTACEI, CON L'ULTERIORE PERICOLO CHE IL LORO SMARRIMENTO (CHE PUÒ ANCHE ESSERE DOVUTO A UN FURTO) PUÒ PASSARE PIÙ FACILMENTE INOSSERVATO. A MENO CHE NON SIATE SICURI CHE CONTENGANO SOLO INFORMAZIONI NON SENSIBILI, RIPONETELI SOTTO CHIAVE NON APPENA AVETE FINITO DI USARLI.
9. *MANEGGIARE E CUSTODIRE CON CURA LE STAMPE DI MATERIALE RISERVATO.* NON LASCIATE ACCEDERE ALLE STAMPE PERSONE NON AUTORIZZATE. SE LA STAMPANTE NON SI TROVA SULLA VOSTRA SCRIVANIA RECA TEVI IL PIÙ IN FRETTA POSSIBILE A RITIRARE LE STAMPE. PER STAMPE RISERVATE CERCATE DI USARE UNA STAMPANTE NON CONDIVISA OPPURE USATE LA MODALITÀ DI STAMPA RITARDATA IMPOSTANDO UN TEMPO SUFFICIENTE A PERMETTERVI DI RAGGIUNGERE LA STAMPANTE PRIMA DELL'INIZIO DELLA STAMPA. DISTRUGGETE PERSONALMENTE LE STAMPE QUANDO NON SERVONO PIÙ O SE ESSE SIANO SOLO DELLE "BRUTTE COPIE" O BOZZE DA RISTAMPARE PERCHÉ ERRATE.
10. *PRESTATE ATTENZIONE ALLE FOTOCOPIE:* FARE FOTOCOPIE DI DOCUMENTI CONTENENTI DATI PERSONALI SENSIBILI SOLO SE STRETTAMENTE NECESSARIO. ASSICURARSI DI NON LASCIARE COPIE NELLA MACCHINA E SE NECESSARIO ELIMINARE COPIE MAL RIUSCITE UTILIZZATE UNA MACCHINA DISTRUGGI-DOCUMENTI (SHREDDER)
11. *NON GETTARE NEL CESTINO LE STAMPE DI DOCUMENTI CHE POSSONO CONTENERE INFORMAZIONI CONFIDENZIALI.* SE TRATTATE DATI DI PARTICOLARE RISERVATEZZA, CONSIDERATE LA POSSIBILITÀ DI DOTARVI DI UNA

MACCHINA DISTRUGGI-DOCUMENTI (SHREDDER). IN OGNI CASO NON GETTATE MAI DOCUMENTI CARTACEI SENZA AVERLI PRIMA FATTI A PEZZI.

12. *NON RIUTILIZZARE I DISCHETTI PER AFFIDARE A TERZI I VOSTRI DATI.* QUANDO UN FILE VIENE CANCELLATO DA UN DISCO MAGNETICO, I DATI NON VENGONO EFFETTIVAMENTE ELIMINATI DAL DISCO MA SOLTANTO MARCATI COME NON UTILIZZATI E SONO FACILMENTE RECUPERABILI. NEANCHE LA FORMATTAZIONE ASSICURA L'ELIMINAZIONE DEI DATI DAI DISCHI. SOLO L'USO DI UN APPOSITO PROGRAMMA DI CANCELLAZIONE SICURA GARANTISCE CHE SUL DISCHETTO NON RESTI TRACCIA DEI DATI PRECEDENTI. NEL DUBBIO, È SEMPRE MEGLIO USARE UN DISCHETTO NUOVO.
13. *PRESTARE PARTICOLARE ATTENZIONE ALL'UTILIZZO DEI COMPUTER PORTATILI.* I PC PORTATILI SONO UN FACILE BERSAGLIO PER I LADRI. SE AVETE NECESSITÀ DI GESTIRE DATI RISERVATI SU UN PORTATILE, PROTEGGETELO CON UNA PASSWORD SUL BIOS, FATE INSTALLARE UN PROGRAMMA DI CIFRATURA DEL DISCO RIGIDO (PER IMPEDIRE LA LETTURA DEI DATI IN CASO DI FURTO) ED EFFETTUATE PERIODICAMENTE IL BACKUP DEI DATI.
14. *PROTEGGERE IL PROPRIO COMPUTER CON UNA PASSWORD. ABILITARE OVE POSSIBILE L'ACCESSO TRAMITE PASSWORD.* LA MAGGIOR PARTE DEI COMPUTER OFFRE LA POSSIBILITÀ DI IMPOSTARE UNA PASSWORD ALL'ACCENSIONE. ANCHE ALCUNI APPLICATIVI PERMETTONO DI PROTEGGERE I PROPRI DATI TRAMITE PASSWORD. IMPARATE A UTILIZZARE QUESTE CARATTERISTICHE CHE OFFRONO UN BUON LIVELLO DI RISERVATEZZA.
15. *FARE ATTENZIONE A NON ESSERE SPIATI MENTRE SI DIGITA UNA PASSWORD O QUALUNQUE CODICE DI ACCESSO.* ANCHE SE MOLTI PROGRAMMI NON RIPETONO IN CHIARO LA PASSWORD SULLO SCHERMO, QUANDO DIGITATE UNA PASSWORD QUESTA POTREBBE ESSERE LETTA GUARDANDO I TASTI CHE STATE BATTENDO, ANCHE SE AVETE BUONE CAPACITÀ DI DATTILOSCRITTURA. CHIEDETE AGLI ASSISTENTI DI GUARDARE DA UN'ALTRA PARTE QUANDO INTRODUCETE UNA PASSWORD O CONTROLLATE CHE NESSUNO STIA GUARDANDO.
16. *NON PERMETTERE L'USO DEL PROPRIO ACCOUNT AD ALTRI COLLEGHI D'UFFICIO.* NON COMUNICATE LA VOSTRA PASSWORD DI ACCESSO AL PC A NESSUNO, NÉ TANTOMENO A COLLEGHI DI UFFICIO. UN'ATTIVITÀ ILLECITA SVOLTA DA UN VOSTRO COLLEGA CON LA VOSTRA PASSWORD SARÀ ATTRIBUITA A VOI, CON TUTTE LE CONSEGUENZE GIURIDICHE DEL CASO.
17. *NON PERMETTERE L'USO DEL PROPRIO COMPUTER O DEL PROPRIO ACCOUNT DA PERSONALE ESTERNO,* A MENO DI NON ESSERE SICURI DELLA LORO IDENTITÀ. PERSONALE ESTERNO PUÒ AVERE BISOGNO DI INSTALLARE DEL NUOVO SOFTWARE/HARDWARE NEL VOSTRO COMPUTER. ASSICURATEVI DELL'IDENTITÀ DELLA PERSONA (ES. TECNICO INFORMATICO INCARICATO DALL'ENTE ALLA MANUTENZIONE DELLE APPARECCHIATURE ELETTRONICHE) E DELLE AUTORIZZAZIONI AD OPERARE SUL VOSTRO PC.
18. *NON UTILIZZARE APPARECCHIATURE NON AUTORIZZATE O PER CUI NON SI È AUTORIZZATI.* L'UTILIZZO DI MODEM SU POSTAZIONI DI LAVORO COLLEGATE ALLA RETE DI UFFICIO OFFRE UNA PORTA D'ACCESSO DALL'ESTERNO NON SOLO AL VOSTRO COMPUTER MA A TUTTA LA RETE DI CUI FATE PARTE. È QUINDI VIETATO L'USO DI MODEM ALL'INTERNO DELLA RETE LOCALE. NEL CASO CHE CIÒ SIA STRETTAMENTE NECESSARIO, DISCONNETTERE FISICAMENTE LA POSTAZIONE DI LAVORO DALLA RETE LOCALE PRIMA DI EFFETTUARE IL COLLEGAMENTO VIA MODEM. PER L'USO DI ALTRE APPARECCHIATURE, CHIEDERE CONSIGLIO AL TITOLARE DEL TRATTAMENTO OPPURE AL RESPONSABILE INFORMATICO.
19. *NON INSTALLARE PROGRAMMI NON AUTORIZZATI.* OLTRE ALLA POSSIBILITÀ DI TRASFERIRE INVOLONTARIAMENTE UN VIRUS O DI INTRODURRE UN COSIDDETTO "CAVALLO DI TROIA", VA RICORDATO CHE LA MAGGIOR PARTE DEI PROGRAMMI SONO PROTETTI DA COPYRIGHT, PER CUI LA LORO INSTALLAZIONE PUÒ ESSERE ILLEGALE.
20. *DIFFIDARE DEI DATI O DEI PROGRAMMI LA CUI PROVENIENZA NON È CERTA.* PER PROTEGGERSI DI VIRUS ED ALTRI AGENTI ATTIVI DI ATTACCO, DIFFIDATE DI TUTTI I DATI E PROGRAMMI CHE VI VENGONO INVIATI O CONSEGNATI, ANCHE SE LA FONTE APPARE AFFIDABILE O IL CONTENUTO MOLTO INTERESSANTE. INFATTI MOLTI SISTEMI DI ATTACCO INVIANO DATI CHE SEMBRANO PROVENIRE DA UN UTENTE NOTO AL DESTINATARIO PER VINCERNE LA NATURALE DIFFIDENZA NEI CONFRONTI DEGLI ESTRANEI.
21. *APPLICARE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DA VIRUS.* LA PREVENZIONE DALLE INFEZIONI DA VIRUS SUL VOSTRO COMPUTER È MOLTO PIÙ FACILE E COMPORTA UNO SPRECO DI TEMPO MOLTO MINORE RISPETTO ALLA CORREZIONE DEGLI EFFETTI DI UN VIRUS. INOLTRE, SE NON AVETE ATTIVATO ADEGUATE MISURE ANTI-VIRUS POTRESTE INCORRERE IN UNA PERDITA IRREPARABILE DI DATI O IN UN BLOCCO ANCHE MOLTO PROLUNGATO DELLA VOSTRA POSTAZIONE DI LAVORO. A TAL FINE, È OPPORTUNO CHE IN OGNI MACCHINA COLLEGATA AD INTERNET VI SIA INSTALLATO UN PROGRAMMA ANTI-VIRUS E CHE TALE PROGRAMMA SIA AGGIORNATO PERIODICAMENTE.
22. *USARE, SE POSSIBILE, IL SALVATAGGIO AUTOMATICO DEI DATI. NON DIMENTICARE I SALVATAGGI VOLONTARI.* MOLTI PROGRAMMI APPLICATIVI, AD ESEMPIO QUELLI DI VIDEOSCRITTURA, SALVANO AUTOMATICAMENTE IL LAVORO A INTERVALLI FISSI, IN MODO DA MINIMIZZARE IL RISCHIO DI PERDITA ACCIDENTALE DEI DATI. IMPARATE COMUNQUE A SALVARE MANUALMENTE IL VOSTRO LAVORO CON UNA CERTA FREQUENZA, IN MODO DA PRENDERE L'ABITUDINE DI GESTIRE VOI STESSI I DATI E NON FARE ESCLUSIVO AFFIDAMENTO SUL SISTEMA.

23. *NON VIOLARE LE LEGGI IN MATERIA DI SICUREZZA INFORMATICA.* RICORDATEVI CHE ANCHE SOLO UN TENTATIVO DI INGRESSO NON AUTORIZZATO IN UN SISTEMA COSTITUISCE UN REATO. SE SIETE INTERESSATI A STUDIARE LA SICUREZZA DELLA VOSTRA POSTAZIONE DI LAVORO O DELLA RETE DI CUI FATE PARTE, CHIEDETE PREVENTIVAMENTE L'AUTORIZZAZIONE AL TITOLARE DEL TRATTAMENTO OPPURE AL RESPONSABILE INFORMATICO. NON UTILIZZATE SENZA AUTORIZZAZIONE SOFTWARE CHE POSSONO CREARE PROBLEMI DI SICUREZZA O DANNEGGIARE LA RETE, COME PORT SCANNER, SECURITY SCANNER, NETWORK MONITOR, NETWORK FLOODER, FABBRICHE DI VIRUS O DI WORM.
24. SEGNALARE TEMPESTIVAMENTE AL TITOLARE O ALL'AMMINISTRATORE DI SISTEMA QUALSIASI VARIAZIONE DEL COMPORTAMENTO DELLA PROPRIA POSTAZIONE DI LAVORO PERCHÉ PUÒ ESSERE IL SINTOMO DI UN ATTACCO IN CORSO.
25. *SEGNALARE COMPORAMENTI CHE POSSANO FAR PENSARE A TENTATIVI DI RIDURRE LA SICUREZZA DEL SISTEMA INFORMATIVO.* AD ESEMPIO SEGNALATE AL RESPONSABILE DELLA SICUREZZA DELL'ENTE SE UN ALTRO UTENTE INSISTE PER AVERE ACCESSO AI VOSTRI DATI O PER CONOSCERE LA VOSTRA PASSWORD O PER POTER LAVORARE SULLA VOSTRA POSTAZIONE DI LAVORO. ANALOGAMENTE NON FIDATEVI E SEGNALATE TELEFONATE O MESSAGGI CHE SEMBRANO PROVENIRE DA UN SISTEMA E VI CHIEDONO DI FARE OPERAZIONI STRANE SUL VOSTRO COMPUTER (AD ESEMPIO, CAMBIARE SUBITO LA PASSWORD CON UNA DATAVI AL TELEFONO O NEL CORPO DEL MESSAGGIO).

per ogni ulteriore informazione sulle modalità di comportamento da tenere sul luogo di lavoro e' necessario far riferimento al titolare del trattamento.