

Norme comportamentali per gli utenti del SISTEMA INFORMATICO DI GESTIONE DOCUMENTALE

PREMESSA

Scopo delle presente documento è indicare le norme comportamentali/tecniche alle quale gli utenti del *Sistema Informatico di gestione Documentale* (d'ora in poi indicato come IRIDE) devono attenersi nello svolgimento delle operazioni di utilizzo del sistema anche in qualità di Incaricati del *trattamento di dati personali* (d'ora in poi indicato come TDP) sotteso ad IRIDE.

In particolare si descrivono:

- i riferimenti normativi relativamente alla Gestione del protocollo informatico, dei flussi documentali e degli archivi
- i riferimenti normativi relativamente agli incaricati sulla base di quanto dispone il *Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali"* (d'ora in poi indicato come CODICE)
- le regole di ordinaria diligenza che da osservare nel corso della prestazione lavorativa
- le misure di sicurezza specifiche da adottare in quanto utenti incaricati all'uso di IRIDE

RIFERIMENTI NORMATIVI - Gestione del protocollo informatico, dei flussi documentali e degli archivi

Il riferimento è il *Manuale di gestione del protocollo informatico, dei flussi documentali e degli archivi* (d'ora in poi MANUALE) approvato con determinazione dirigenziale DN-12/490 del 12.5.2015 in ottemperanza agli sensi degli articoli 3 e 5 del D.P.C.M. 3.12.2013 "Regole tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del CAD" e sulla base degli indirizzi di gestione documentale di cui alla deliberazione di Giunta Comunale n. 4 del 14.1.2014.

Si ricordano gli articoli del MANUALE che interessano per l'identificazione dei ruoli gestionali previsti in IRIDE

Art. 3 - Area Organizzativa Omogenea (AOO)

1. Per la gestione unica e coordinata dei documenti, l'Amministrazione individua un'unica Area Organizzativa Omogenea (AOO) denominata Comune di Pisa ...

Art. 4 - Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi

1. Ai sensi della normativa vigente, l'Amministrazione istituisce il Servizio per la tenuta del protocollo informatico, la gestione dei flussi documentali e degli archivi, individuandolo nell'Ufficio Gestione Documentale cui afferiscono le funzioni del Protocollo e dell'Archivio.
2. Al Servizio è preposto il Responsabile dell'Ufficio Gestione Documentale per l'AOO Comune di Pisa.

Art. 9 Responsabile della gestione documentale

2. Il Responsabile della Gestione documentale provvede a:
 - a. individuare gli utenti ed attribuire loro un livello di autorizzazione all'uso di funzioni della procedura, distinguendo quelli abilitati alla mera consultazione dell'archivio, o di parti di esso, da quelli abilitati anche all'inserimento, modifica e aggiunta di informazioni; ...

Art. 11 - Accessi differenziati

2. Gli operatori interni del servizio di protocollo hanno autorizzazioni di accesso differenziate in base alle tipologie di operazioni.
3. Ad ogni operatore è assegnata una "login" ed una "password" d'accesso al sistema informatico di gestione del protocollo. Ogni operatore, identificato dalla propria login, dal sistema informatico di gestione del protocollo, è responsabile della corrispondenza dei dati desunti dal documento protocollato con quelli immessi nel programma di protocollo, e della corrispondenza del numero di protocollo di un documento all'immagine o file del documento stesso archiviato nel sistema informatico.
4. I livelli di autorizzazione sono assegnati dal Responsabile della Gestione documentale di cui all'art. 9 secondo i principi contenuti nel presente provvedimento. ...

Articolo 16 - Accessibilità da parte degli utenti appartenenti all'AOO

2. Ogni utente è associato un ruolo (scrivania virtuale). Ogni ruolo ha la possibilità di accedere solo ai documenti di competenza della propria scrivania virtuale e può creare e gestire solo i propri fascicoli virtuali.
3. Il livello di riservatezza applicato ad un fascicolo è ereditato automaticamente da tutti i documenti in esso inseriti.

RIFERIMENTI NORMATIVI – Incaricati del TDP

Nell'ambito di IRIDE è presente la problematica della gestione di dati personali, sia in quanto presenti nei dati archiviati nel sistema (es. i dati di protocollo) sia in quanto presenti nei documenti allegati.

Il concetto di "dato personale" (art. 4, comma 1, lett. b del CODICE) fa riferimento a qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

Le figure prese in considerazione dal CODICE (qui già riportate alla realtà del Comune) sono:

- Interessato: la persona fisica, cui si riferiscono i dati personali
- Titolare: la persona giuridica cui competono le decisioni in ordine alle finalità, alle modalità del TDP e agli strumenti utilizzati, ivi compreso il profilo della sicurezza
- Responsabile: la persona fisica preposto dal Titolare al trattamento di dati personali
- Incaricati: le persone fisiche autorizzate a compiere operazioni di TDP dal Responsabile;

Le operazioni di TDP (art. 30 del CODICE) possono essere effettuate solo da Incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni impartite dallo stesso.

Il Comune di Pisa con delibera di Consigli Comunale n. 1 del 12.1.2006 ha approvato il *Regolamento per l'accesso ai documenti e alle informazioni e per la tutela dei dati personali* che ha dettato queste norme (per gli aspetti che qui interessano):

ART. 19 - Titolare, Responsabili, Incaricati ed Interessati

1. *Il Comune di Pisa è il Titolare dei trattamenti dei dati personali gestiti dalle proprie articolazioni organizzative ...*
2. *I dirigenti, ... sono Responsabili dei trattamenti dati personali afferenti alla struttura a loro assegnata.*
3. *I Responsabili garantiscono l'applicazione di quanto previsto dal D.Lgs. 196/03 e dal presente regolamento sul trattamento dei dati di competenza ...*
In particolare provvedono, in relazione alle strutture di propria competenza:
 - a designare i dipendenti che sono incaricati del trattamento dei dati
 - ad impartire ai suddetti incaricati le istruzioni sulle modalità del trattamento dati, in conformità a quanto previsto dall'art.30 comma 2 del D.Lgs. 196/03, vigilando sulle operazioni da loro effettuate; ...
 - ad applicare le misure organizzative di propria competenza che vengano indicate dal Dirigente del Sistema Informativo ai sensi del successivo comma 4.
4. *Il Dirigente del Sistema Informativo è Responsabile, altresì:*
 - dell'applicazione delle misure sotto il profilo della sicurezza delle infrastrutture hardware, software e di comunicazione sottese ai trattamenti dati personali effettuati nel Comune di Pisa ai sensi di quanto previsto dagli artt. 33-36 del D.Lgs. 196/03; ...

In data 29.1.2004 il Dr. Paoli Luigi, in qualità di Dirigente della Direzione Sportello al Cittadino e Sistema Informativo, indirizzò a tutti i dipendenti autorizzati all'accesso di IRIDE le istruzioni agli incaricati del TDP ai sensi di quanto previsto dal CODICE.

Con questo documento si intende aggiornare anche le suddette istruzioni alla luce delle modifiche normative intervenute e delle evoluzioni tecnologiche del sistema IRIDE.

NORME COMPORTAMENTALI per l'uso di IRIDE

Il documento è firmato da:

-Paoli Luigi in quanto dirigente della Direzione Programmazione, Organizzazione, Sistema Informativo e, pertanto, responsabile sotto il profilo della sicurezza delle infrastrutture hardware, software e di comunicazione del Comune di Pisa

-Geri Patrizio in quanto Posizione Organizzativa Ufficio Gestione Documentale e, pertanto, Responsabile della Gestione Documentale del Comune di Pisa e delegato Responsabile del TDP sotteso a IRIDE.

Questo documento ha valenza di istruzioni ai dipendenti/amministratori comunali autorizzati all'accesso a IRIDE e, quindi, Incaricati al relativo TDP ai sensi del CODICE.

*L'utente di IRIDE anche nella sua qualità di Incaricato al TDP sotteso ad IRIDE (di seguito indicato per brevità solo con *Utente*) dovrà scrupolosamente attenersi alle presenti istruzioni.*

Le regole di ordinaria diligenza dell'incaricato

I documenti e i dati comunque legittimamente conosciuti, acquisiti, utilizzati, nell'esercizio delle attività di competenza dovranno essere trattati in modo lecito e secondo correttezza; raccolti, registrati e conservati per gli scopi determinati, espliciti e legittimi propri della struttura alla quale l'*Utente* è assegnato o dell'incarico che gli è stato affidato.

Deve essere garantita la massima riservatezza sui documenti e sui dati dei quali l'*Utente* venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso.

E' tassativamente vietato l'uso improprio dei documenti e dei dati personali di cui l'*Utente* venga a conoscenza.

L'*Utente* potrà procedere alla comunicazione/diffusione di documenti e di dati personali solo se questo costituisca oggetto di uno specifico compito affidato.

L'*Utente*, pertanto, deve prestare particolare attenzione nel:

- non divulgare a terzi estranei le informazioni di cui viene a conoscenza
- adoperarsi affinché terzi fraudolentemente non entrino in possesso dei dati/documenti
- non fare copie, per uso personale, dei dati/documenti su cui svolgono operazioni di ufficio
- trattare i dati personali per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- non effettuare accessi non autorizzati o di trattamento non consentito o non conforme alle finalità proprie dell'attività lavorativa
- in caso di abbandono temporaneo della propria postazione di lavoro, provvedere ad attivare il salva schermo del personal computer con password.

Misure di sicurezza specifiche di IRIDE

- I codici di identificazione individuali per l'accesso ad IRIDE non devono mai essere condivisi tra più *Utenti*. Nel caso altri *Utenti* debbano poter accedere ai dati è necessario che il Dirigente di riferimento richieda l'autorizzazione al Responsabile della Gestione Documentale.
- Le password devono essere sostituite, a cura del singolo *Utente*, almeno ogni sei mesi.
- Per una corretta gestione delle password, ciascun *Utente* deve avere cura di:
 - impostare la password con una lunghezza di almeno 8 caratteri, salvo diverse istruzioni
 - non trascriverla su fogli, agendine, post-it facilmente accessibili a terzi
 - in caso di modifica della password, non utilizzare le precedenti 5
 - sostituirla immediatamente nel caso di perdita della sicurezza della stessa
 - non basarla su informazioni facilmente deducibili, quali il proprio nome, il nome dei familiari, la data di nascita, il proprio codice fiscale
 - non includere la password in alcun processo di connessione automatica.

In caso di revoca/esclusione dall'incarico che consentiva l'accesso a IRIDE il relativo codice di identificazione individuale viene a decadere con decorrenza immediata

Sono previste scrivanie virtuali "individuali" solo nel caso dei Dirigenti, Posizioni Organizzative, Sindaco, Assessori.

La scrivania virtuale individuale non potrà avere più di due *Utenti* autorizzati all'accesso:

-il dipendente titolare della scrivania virtuale

-un altro dipendente con poteri sostitutivi del titolare; questo dipendente deve essere segnalato dal "titolare" della scrivania virtuale al Responsabile della gestione documentale che provvederà alla relativa abilitazione.

Entro il giorno 18 aprile p.v. i titolari delle scrivanie virtuali comunicheranno al Responsabile della Gestione Documentale il nominativo del sostituto.

Dal giorno 19 aprile p.v. tutte gli altri *Utenti* diversi dal titolare/sostituto saranno disabilitati all'accesso di una scrivania virtuale individuale.

I dati di protocollo non devono contenere dati personali sensibili o giudiziari ai sensi del CODICE. Pertanto l'*Utente* che registra il protocollo avrà cura di riportare una descrizione nei campi Tipologia documento, Oggetto, Mittente/Destinatario tali da garantire la "non esposizione" di dati sensibili o giudiziari ai sensi del CODICE.

Con la presente si ricorda che il CODICE prevede sanzioni nel caso di inottemperanza delle regole sul TDP e delle relative misure di sicurezza; in particolare sono previste sanzioni penali per chi procede ad un TDP al fine di trarre profitto per sé e per altri o al fine di recare un danno ad altri. Infine è previsto che chiunque cagiona danno ad altri per effetto del TDP è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

PAOLI Luigi



GERI Patrizio

