REGISTRO UNICO ATTIVITA' E CATEGORIE DI ATTIVITA' DEL TRATTAMENTO PER LA PROTEZIONE DEI DATI PERSONALI EX ART. 30 REG.UE 2016/679	SETTORE n. banca-dati n.

STRUTTURA DI COMPETENZA	
settore n.	
servizio	
ufficio	

TITOLARE TRATTAMENTO	COMUNE DI	**RESPONSABILE TRATTAMENTO**	Dirigente del Settore n.
indirizzo		**indirizzo**	
telefono n.		**telefono n.**	
mail		**mail**	
PEC		**PEC**	
CONTITOLARE TRATTAMENTO		**RESPONSABILE PROTEZIONE DATI**	
indirizzo		**indirizzo**	
telefono n.		**telefono n.**	
mail		**mail**	
PEC		**PEC**	

BANCA DATI	
nome	
tipologia	□ informatica □ cartacea □ mista □ visiva/audio-visiva □ *(altra)*
ubicazione	
strumenti elettronici utilizzati	
tipologia	□ p.c. in rete □ p.c. in rte interna o VPN □ p.c. in rete esterna □ *(altro)*
interconnessione	tipologia: □ LAN □ VPN □ geografica
backup	frequenza obbligatoria: □ giornaliera □ settimanale □ mensile □ *(altro)*
responsabile backup	
luogo conservazione copia di backup	□ stanza munita di serratura □ stanza aperta □ cassaforte interna all'ufficio □ armadio di sicurezza □ armadio ignifugo □ armadio/schedario/cassetto munito di serratura □ *(altro)*
responsabile backup	
strumenti non elettronici utilizzati	
contenitori muniti di serratura: □ armadio □ armadio ignifugo □ schedario □ cassaforte □ armadio semiblindato	

TRATTAMENTO	
Descrizione[(1)] attività	
finalità trattamento	
fonte normativa	
Operazioni[(2)] di trattamento da eseguire	raccolta – registrazione – organizzazione – strutturazione – conservazione - adattamento modifica – estrazione – consultazione – uso – comunicazione tramite trasmissione - diffusione o qualsiasi altra forma di messa a disposizione - raffronto o interconnessione – limitazione - cancellazione o distruzione
destinatari	

(1) Sintetica - (2) Cancellare le operazioni da non attuare

REGISTRO UNICO ATTIVITA' E CATEGORIE DI ATTIVITA' DEL TRATTAMENTO PER LA PROTEZIONE DEI DATI PERSONALI EX ART. 30 REG.UE 2016/679	SETTORE n. banca-dati n.

TRASMISSIONE VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI
(specificare)

CATEGORIE DI INTERESSATI E DATI								
categorie interessati		cittadini residenti		elettori		utenti		chiunque
		componenti organi di governo del titolare o di altri soggetti giuridici						
		dipendenti del titolare				collaboratori del titolare		
		appartenenti a partiti politici, sindacati, associazioni, fondazioni, comitati, ecc.						
		(altri: specificare)						
categorie dati		sensibili		giudiziari		non sensibili e non giudiziari		
consenso		no		si *(soltanto se sussiste un obbligo di legge)*				
termine ultimo per cancellare i dati *(soltanto se previsto da una norma giuridica)* :								

RISCHI						
codice	**rischi**	**sussiste**		**gravità impatto**		
		si	**no**	**bassa**	**media**	**alta**
	A - rischi relativi ai comportamenti degli operatori					
RA.1	sottrazione di credenziali di autenticazione					
RA.2	carenza di consapevolezza, disattenzione e incuria					
RA.3	comportamenti sleali o fraudolenti					
RA.4	errore materiale					
RA.5	*(altro)*					
RA.6	*(altro)*					
	B - rischi relativi agli strumenti					
RB.1	azione di virus informatici o di programmi suscettibili di recare danno					
RB.2	spamming o tecniche di sabotaggio					
RB.3	malfunzionamento, indisponibilità o degrado degli strumenti					
RB.4	accessi esterni non autorizzati					
RB.5	intercettazione di informazioni in rete					
RB.6	*(altro)*					
RB.7	*(altro)*					
	C - rischi relativi al contesto					
RC.1	accessi non autorizzati a locali/reparti ad accesso					
RC.2	sottrazione di strumenti contenenti dati					
RC.3	eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria					
RC.4	guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.)					
RC.5	errori umani nella gestione della sicurezza fisica					
RC.6	*(altro)*					
RC.7	*(altro)*					

MISURE					
codice	**tipologia**	**descrizione sintetica**	**elementi descrittivi**	**attuate [1] si**	**no**
M.001	fisica	impianto di allarme	gli spazi interessati alla misura sono dotati di impianto di allarme in grado di rilevare e segnalare l'eventuale intrusione di soggetti non autorizzati		
M.002	fisica	sistema antincendio	gli spazi interessati alla misura sono dotati di impianto di antincendio in grado di fronteggiare situazioni di emergenza		
M.003	fisica	inferriate o blindature alle vie di accesso alla sala server	la via di accesso agli spazi interessati alla misura è dotata di protezione fisica tipo inferriate o blindature in grado di impedire o comunque rendere difficile l'ingresso agli stessi senza la disponibilità della relativa chiave.		
M.004	fisica	porte chiudibili a chiave per tutti gli uffici e gli archivi	l'accessibilità agli spazi interessati alla misura è assoggettata alla utilizzazione di una apposita chiave disponibile solo per i soggetti appositamente autorizzati.		
M.005	fisica	armadi a pareti ignifughe	per la protezione da danni derivanti da incendi viene utilizzato un tipo di armadio di contenimento con pareti in grado di resistere al fuoco ed alle alte temperature per un tempo sufficiente a porre in sicurezza i contenuti dello stesso prima del loro deterioramento.		
M.006	fisica	estintori	I locali sono dotati di appositi estintori		
M.007	fisica	Climatizzatore per la sala server	Il locale o vano oggetto della protezione è opportunamente climatizzato per poter assicurare il mantenimento di temperature operative compatibili durante tutto il periodo dell'anno.		
M.008	fisica	Armadi e cassettiere chiudibili a chiave	l'accessibilità agli armadi e cassettiere interessati alla misura è assoggettata alla utilizzazione di una apposita chiave disponibile solo per i soggetti appositamente autorizzati		
M.009	fisica	gruppo statico di continuità (UPS)	Il carico elettrico da proteggere è alimentato attraverso un gruppo statico di continuità in grado di erogare, senza interruzione, la potenza elettrica necessaria per un tempo sufficiente a porre in sicurezza il carico stesso.		
M.010	fisica	linea elettrica dedicata	Al fine di eliminare interruzioni al carico da proteggere derivanti da problemi relativi al alti carichi. Questi viene alimentato con linea elettrica separata e dedicata dal quadro generale più vicino.		
M.011	fisica	password condivisa di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso.		
M.012	fisica	password personale di accesso alla stazione	L'accesso alla risorsa fisica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto dalla sola persona a cui è stato affidato da parte dell'Amministratore del sistema.		
M.013	logica	password condivisa di accesso alla stazione	L'accesso alla procedura informatica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto da più persone abilitate all'accesso.		
M.014	logica	password personale di accesso alla stazione	L'accesso alla procedura informatica in questione è assoggettato alla conoscenza di una password sufficientemente robusta e costituita da un segreto conosciuto dalla sola persona a cui è stato affidato da parte dell'Amministratore del sistema.		

M.015	fisica	sistema di autorizzazione basato su profili	Il modulo software utilizzato per il trattamento dei dati oggetto della misura di protezione è basato su un sistema di profilazione dell'utenza che prevede di differenziare le possibili operazioni di trattamento eseguibili dai vari utenti in base al profilo/i specifico/i ad essi assegnati.		
M.016	logica	logging	L'accesso alla risorsa informatica in questione è assoggettato a tracciature delle operazioni effettuate con la registrazione di: - epoca dell'operazione - indirizzo di rete della stazione accedente (se definito) - descrizione dell'operazione fatta - identificativo dell'utente che compie l'operazione Tali file di log sono accuratamente conservati per l'eventuale loro controllo		
M.017	organizzativa	backup	I dati o programmi in questione sono copiati con regolarità su supporti fisici diversi che sono poi conservati in locali separati opportunamente protetti da accessi non autorizzati.		
M.018	organizzativa	copie multiple	Le procedure di backup sono effettuate producendo copie multiple che sono poi conservate in locali diversi ciascuno soggetti ad opportune restrizioni di accesso.		
M.019	logica	cancellazione dei supporti fisici contenenti dati non più necessari	Il supporto fisico contenente i dati in questione che non risultano più necessari e quindi oggetto di protezione, viene cancellato mediante le opportune tecniche dipendenti dalla natura del supporto stesso. Tali operazioni di cancellazioni renderanno il contenuto di tale supporto non più leggibile con strumenti informatici di normale uso in ambito informatico.		
M.020	organizzativa	informazione/formazione specifica sul rischio	Gli incaricati del trattamento sulla banca oggetto della misura sono stati resi edotti, in modo specifico e puntuale, degli eventi dannosi relativi a quella banca dati e sulle misure adottate per contrastare il rischio derivante. Sono state poi date istruzioni operative dettagliate sul come rendere operative le misure di contrasto del rischio.		
M.021	organizzativa	antivirus	Sui sistemi interessati al trattamento dei dati in questione sono stati installati opportuni software di protezione dai virus informatici. Tali software sono costantemente aggiornati, in modo automatico, con frequenza almeno giornaliera. In certe situazioni il sistema provvede ad aggiornamenti più frequenti.		
M.022	organizzativa	modifica periodica delle credenziali	Le credenziali di accesso, quali password o certificati digitali, vengono rinnovate con una frequenza idonea a garantire le banche dati accedute da utilizzo delle stesse da parte di soggetti non autorizzati che abbino sottratto o generato, con opportune procedure di password-cracking, le stesse.		
M.023	organizzativa	Password dello screen saver	Quando la postazione di lavoro è lasciata incustodita, si avvia in automatico dopo un intervallo di tempo, lo screen saver. La disattivazione dello screen saver richiede l'inserimento di una password		

(1) Contrassegnare con la x soltanto le misure attuate nella colonna "si" e le misure da attuare nella colonna "no". Sbarrare le caselle le cui misure non sono comunque da attuare.

REGISTRO UNICO ATTIVITA' E CATEGORIE DI ATTIVITA' DEL TRATTAMENTO PER LA PROTEZIONE DEI DATI PERSONALI EX ART. 30 REG.UE 2016/679	SETTORE n. banca-dati n.

TRATTAMENTI ESTERNALIZZATI						
Soggetto esterno affidatario	– **estremi identificativi e sede legale:** – **sede del trattamento:** – **ruolo ai fini del trattamento:** □ contitolare □ responsabile					
Attività esternalizzata	– **attività affidate comportanti il trattamento dati:** (*indicarle sinteticamente)* – **estremi degli atti e contratto di affidamento:**					
Natura dei dati		**sensibili**		**giudiziari**		**non sensibili e non giudiziari**
Operazioni [(1)] di trattamento da eseguire	raccolta – registrazione – organizzazione – strutturazione – conservazione - adattamento modifica – estrazione – consultazione – uso – comunicazione tramite trasmissione - diffusione o qualsiasi altra forma di messa a disposizione - raffronto o interconnessione – limitazione - cancellazione o distruzione					
Criteri e impegni [(2)] assunti per l'adozione delle misure	Nella ipotesi che con l'atto di affidamento del servizio esternalizzato non siano stati definiti, a norma del regolamento approvato dalla Giunta Comunale n. 165 del 13/05/2003, il ruolo – titolare o responsabile del trattamento – nonché determinati i dati personali trattabili e le operazioni di trattamento eseguibili, è necessario che il soggetto a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni anche su base contrattuale, con particolare riferimento, ad esempio, a: 1. trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto; 2. adempimento degli obblighi previsti dal Codice per la protezione dei dati personali; 3. rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere; 4. impegno a relazionare periodicamente sulle misure di sicurezza adottate anche mediante eventuali questionari e liste di controllo- e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.					

(1) cancellare le operazioni da non attuare

(2) modificare secondo quanto previsto nell'atto o contratto di affidamento del servizio

data, ...

IL RESPONSABILE DEL TRATTAMENTO

.....

IL SUB-RESPONSABILE DEL TRATTAMENTO

.....

REGISTRO UNICO ATTIVITA' E CATEGORIE DI ATTIVITA' DEL TRATTAMENTO PER LA PROTEZIONE DEI DATI PERSONALI EX ART. 30 REG.UE 2016/679	SETTORE n. banca-dati n.

INDICAZIONI PER LA REDAZIONE:

settore: *la numerazione segue quella della struttura organizzativa del Comune;*

banca-dati: *il numero è dato secondo l'ordine attribuito dal dirigente del settore, in modo da avere un ordine che consenta con facilità la sua individuazione e per gli aggiornamenti della stessa;*

*"**banca-dati**": qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;*

*indicare la **finalità perseguita** e l'**attività svolta** (es.: richiesta/trasferimento residenza, contrazione matrimonio, dichiarazione di nascita, dichiarazione di morte, leva, a.i.r.e., autorizzazioni commercio fisso, autorizzazione commercio ambulante, fornitura di beni o servizi, affidamento lavori pubblici, gestione del personale, permessi di costruzione, D.I.A. per costruzioni edilizie, D.I.A. per attività commerciali, autorizzazioni occupazione suolo pubblico, erogazione di contributi, prestito libri, contravvenzioni al codice della strada, contravvenzioni alla normativa sul commercio, soggiorni climatici per minori, contenzioso amministrativo/giurisdizionale civile/amministrativo, amministratori comunali, procedimenti disciplinari, trattamento giuridico e/o economico personale dipendente, cessione quote sindacali dipendenti, contrazione mutui INPDAP, ecc.);*

indicare la/le categoria di persone fisiche individuali o appartenenti a persone giuridiche pubbliche o private i cui dati sono oggetto di trattamento;

*"**fonte normativa"** in base alla quale è svolto il procedimento amministrativo, nel cui ambito sono trattati i dati personali;*

***"dati comuni"** sono i dati non rientranti nelle categorie dei dati sensibili e dai dati giudiziari;*

*"**dati sensibili**" sono i dati personali idonei a rivelare : l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;*

*"**dati giudiziari**" sono i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;*