REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Sommario

1. Scopo e ambito di applicazione 3

2. Definizioni 3

2.1 GDPR 3

2.2 I riferimenti nel GDPR 5

3. Data mapping e definizione dei ruoli 5

3.1 Organigramma Privacy 6

3.2 Trattamenti 6

4. Sistemi Informativi 44

4.1 Approccio basato sul rischio 44

4.2 Applicativi: Privacy by Design e Privacy by Default 44

4.3 Misure di Sicurezza 45

4.4 Valutazione dei rischi generali 48

4.5 Accessi non autorizzati alla struttura 48

4.6 Incendio 48

4.7 Distruzione o perdita dei dati cartacei 48

4.8 Divulgazione dati a soggetti non autorizzati 49

4.9 Contagio da virus informatici 49

4.10 Accessi non autorizzati da rete esterna 49

4.11 Condotte degli operatori 49

5. Contrattualistica Privacy 51

6. MOG- Privacy 51

7. Integrazione Informative 52

8. Audit sulle misure tecniche ed organizzative 52

9. Revisione 53

10. Sottoscrizione 53

Data	Edizione	Redattore/i	Descrizione
	I		Prima redazione

1. Scopo e ambito di applicazione

Il presente Registro delle attività di trattamento, ivi comprensivo di tutti i suoi allegati è predisposto dall'Ente, **Comune di Medolla**, con sede in (41036) Medolla (MO), Piazza della Repubblica 1, nella sua qualità di Titolare del trattamento al fine di:

- consuntivare e storicizzare i trattamenti di dati personali effettuati dall'Ente nonché ogni altra attività relativa alla gestione delle informazioni connesse al perseguimento dei fini istituzionali;
- fornire all'Ente, ai suoi dipendenti, alle eventuali risorse in distacco e anche ai consulenti esterni, istruzioni organizzative e tecniche che consentano l'osservanza degli obblighi e, quindi, il rispetto delle prescrizioni previste dall'attuale normativa in materia di protezione dei dati personali;
- delineare il quadro di sicurezza del sistema informativo e di affidabilità dei relativi programmi informatici ai fini della tutela dei dati personali trattati;
- avere piena coscienza del grado d'esposizione del proprio patrimonio informativo ai rischi specifici come individuati dalla normativa in materia di protezione del dato personale, in modo da poter applicare le misure di sicurezza atte a garantire la protezione dei dati trattati soprattutto attraverso gli strumenti elettronici;
- dimostrare il percorso di adeguamento effettuato per garantire la compliance al Regolamento Europeo (UE) 2016/679 (per il prosieguo, anche solo "GDPR" o "Regolamento").

Tanto premesso, si chiarisce fin da ora che il Registro, oltre a rispondere ai requisiti richiesti dal GDPR, vuole costituire uno strumento utile, in ottica di *accountability*, atto ad illustrare il percorso e gli adempimenti posti in essere dal Titolare, monitorarli ed aggiornarli, anche in modo da garantire l'adeguatezza delle misure tecniche ed organizzative implementate.

2. Definizioni

2.1 GDPR

Di seguito vengono riportate le definizioni indicate dall'art. 4 del GDPR delle quali bisogna tener conto nel presente documento.

«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;

«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

«archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

«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;

«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

«rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

«amministratore si sistema»: le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi

2.2 *I riferimenti nel GDPR*

Considerando n. 82

"Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti".

Art. 30 GDPR – Registri delle attività di trattamento

"1.Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

3.I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.

4.Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5.Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10".

3. Data mapping e definizione dei ruoli

Tenuto conto di quanto già implementato per l'osservanza del D. Lgs. 196/2003 nonché dei provvedimenti dell'Autorità Garante per la protezione dei dati personali, dell'organizzazione dell'Ente e dei relativi ruoli e del personale autorizzato alle attività di trattamento di dati personali, il Titolare ha preliminarmente intrapreso un'attività di data mapping.

Quest'ultima è stato effettuata attraverso specifici incontri dedicati al tema della *data protection,* attraverso la partecipazione dei soggetti interni e/o esterni all'Ente, che hanno contribuito ad identificare e categorizzare le attività di trattamento svolte dal Titolare.

Oltre che alle differenti tipologie di dati trattati all'interno delle diverse aree e al relativo flusso interno ed esterno, tale attività ha permesso anche di individuare i processi di lavoro e le relative modalità di esecuzione comprensiva dei sistemi coinvolti, così da avere un quadro generale ed esaustivo preliminare che ha permesso di determinare quali attività di adeguamento necessitassero di implementazione.

3.1 Organigramma Privacy

A seguito delle attività di data mapping, il Titolare ha implementato un organigramma privacy idoneo ad assicurare una corretta gestione dei dati e dei trattamenti rispetto ai vari settori e alle aree di interesse di cui si compone l'Ente.

RIFERIMENTI DOCUMENTALI

- Organigramma privacy

Una volta individuati i soggetti interni (come da Organigramma Privacy), gli stessi sono designati e/o autorizzati al trattamento mediante appositi atti di nomina in osservanza di quanto previsto dall'art. 29 del GDPR per cui "*chiunque agisca sotto l'autorità del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*".

Gli atti di nomina sono stati formalizzati tenendo conto:

- delle categorie di dati trattati;
- dei trattamenti effettuati;
- del ruolo ricoperto all'interno dell'organizzazione del Titolare.

Resta inteso che l'impostazione descritta tiene conto anche delle scelte a cui il Titolare ha dato seguito considerando il ruolo e il supporto offerto dal Data Protection Officer.

3.2 Trattamenti

L'attività di data mapping, unitamente all'analisi degli applicativi utilizzati dal Titolare per compiere le operazioni di trattamento, ha permesso di individuare le categorie di interessati a cui si riferiscono i dati personali e quelle di destinatari a cui i dati personali sono o saranno comunicati, nonché, laddove sussistenti, i trasferimenti dei dati all'estero.

Si vedano in merito le seguenti tabelle.

Commentato [CF1]:

DIPENDENTI E COMANDATI/DISTACCATI	Interessati con i quali il Titolare ha instaurato un contratto di lavoro	
Tipologie dati trattati	• comuni • particolari (ex artt. 9 e 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • curriculari • idonei a rivelare lo stato di salute (es. documentati in certificazioni mediche o comunicati in caso di infortunio e di incidenti o in dipendenza dell'appartenenza alle categorie protette in osservanza della Legge n. 68/1999 e s.m.i.) e ulteriori dati particolari (es. origine etnica, appartenenza a sindacati e a partiti politici etc.) • retributivi (ivi incluse le trattenute per iscrizione al sindacato) contabili e fiscali • relativi a condanne penali/reati e/o a connesse misure di sicurezza • relativi alle sanzioni amministrative del personale addetto agli automezzi • informatici derivati dall'accesso al sito web, alle caselle di posta elettronica, agli applicativi e alle piattaforme di pertinenza dell'Ente e messi a disposizione del personale autorizzato ai trattamenti da esso svolti e dipendenti dalle attività affidate • relativi alle prestazioni lavorative/professionali • relativi alle valutazioni delle performance	
Finalità necessarie e relative basi giuridiche	Gestione del rapporto lavorativo Adempimento di specifici obblighi in dipendenza delle garanzie in materia di ambiente e sicurezza (es. D.lgs. n. 81/2008) Adempimento degli obblighi di legge conseguenti (es. contratti collettivi pubblico impiego, D.lgs. n. 165/2001, D.lgs. n. 75/2017, Direttiva n. 3/2018, Legge n. 104/1992, Legge n. 68/99 e D.lgs. n. 151/2015, legge n. 241/1990 e regolamenti comunali di interesse Adempimento di specifiche garanzie di legge (art. 54 del D.lgs. n. 165/2001) Gestione richiami disciplinari in base alla normativa applicabile Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (valutazione della prestazione lavorativa)	Dati di performance professionali per la valutazione della prestazione lavorativa	**Base giuridica del trattamento:** adempimento obblighi di legge di cui al D.lgs. n. 150/2009
Trattamento per finalità ulteriori (diffusione)	Dati personali di interesse di cui al fascicolo del personale	**Base giuridica del trattamento:** adempimento obblighi di legge di cui al D.lgs. n. 33/2013 Adempimento obblighidipendenti dalla messa in opera delle banche dati pubbliche (es.PerlaPA)

DIPENDENTI E COMANDATI/DISTACCATI	Interessati con i quali il Titolare ha instaurato un contratto di lavoro	
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse di cui al fascicolo del personale	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Trattamento per finalità ulteriori (Whistleblowing)	Dati identificativi	**Base giuridica del trattamento:** adempimento specifiche garanzie di legge per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione (art. 54 – bis del D.lgs. n. 165/2001e.s.m.i.)
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti legali e fiscali e giuslavoristici • Formatori • Istituti di credito • Provider servizi informatici • Compagnie assicuratrici • Professionisti in ambito sanitario (D.lgs. n. 81/2008) • RSPP • ANAC • Enti pubblici (es. Inps e Inail) • Sindacati di riferimento • Amministrazione finanziaria • Unione Comuni del Modenese Area Nord (UCMAN) • Nucleo di Valutazione • Polo archivistico regionale e archivio comunale • Banche dati pubbliche (es. PerlaPA)	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

Commentato [CF2]: Se esterno

Commentato [CF3]: Da confermare

Commentato [CF4]: Da confermare

STAGISTI	Interessati i cui dati sono trattati per lo svolgimento delle attività di tirocinio/stage formativo
Tipologie dati trattati	• comuni • particolari (ex art. 9 del GDPR)
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • curriculari • contabili e fiscali • informatici derivati dall'accesso al sito web, alle caselle di posta elettronica, agli applicativi e alle piattaforme di pertinenza dell'Ente e messi a disposizione del personale autorizzato ai trattamenti da esso svolti e dipendenti dalle attività affidate • idonei a rivelare lo stato di salute (es. in dipendenza dell'appartenenza alle categorie protette di cui alla Legge n. 68/2009 e s.m.i.), o altri dati di natura particolare, anche nel caso questi comunicati per il tramite del curriculum • relativi all'attività prestata
Finalità necessarie e relative basi giuridiche	Gestione dell'attività di tirocinio/stage formativo Adozione provvedimenti amministrativi e gestione relativi procedimenti Adempimento degli obblighi di legge conseguenti (D. Lgs n. 267/2000, Legge n 241/1990, D.P.R. n. 445/2000; D.M. n. 2/2005 e linee guida nazionali sui tirocini formativi, Legge n. 68/2009 e i regolamenti comunali di interesse Adempimento di specifiche garanzie in materia di ambiente e sicurezza (es. D.lgs. n. 81/2008 e il codice di comportamento di cui all'art. 54 del D.lgs. n. 165/2001 Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo
Destinatari dei dati e/o terzi	• Consulenti legali e in materia contabile e fiscale • Istituti di credito • Provider servizi informatici • RSPP • Enti pubblici (es. Inps e Inail) • Unione Comuni del Modenese Area Nord (UCMAN) • Formatori • Università, Istituti scolastici o altri enti convenzionati, cooperative sociali con cui intercorrono gli accordi per lo svolgimento di stage e tirocini formativi
I dati sono trasferiti extra UE	No
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto

Commentato [CF5]:

Commentato [CF6]:

Commentato [CF7]:

ORGANIZZAZIONE ENTE (es. Amministratori e Sindaco)	Soggetti che rivestono funzioni di rappresentanza e/o ricoprono cariche istituzionali	
Tipologie dati trattati	• comuni • particolari (ex artt. 9 e 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • curriculari • contabili e fiscali • idonei a rivelare lo stato di salute (e ulteriori dati particolari (es. appartenenza a sindacati e a partiti politici etc.) • relativi a condanne penali, reati e/o connessi a misure di sicurezza • informatici derivati dall'accesso al sito web, alle caselle di posta elettronica, agli applicativi e alle piattaforme di pertinenza dell'Ente	
Finalità necessarie e relative basi giuridiche	Esecuzione e gestione del rapporto in essere Adempimento degli obblighi di legge che ne conseguono (es. contratti collettivi pubblico impiego, leggi elettorali, D.lgs. n. 267/2000; D.lgs. n. 165/2001, Legge n. 190/2012, D.lgs. n. 82/2005, D.lgs. n. 241/1990, D.P.R. n. 445/2000 Legge n. 68/99 e D.lgs. n. 151/2015, e regolamenti comunali) Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento per finalità ulteriori (diffusione)	Dati personali di interesse di cui al fascicolo dell'interessato	**Base giuridica del trattamento:** adempimento obblighi di legge di cui al D.lgs. n. 33/2013
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse di cui al fascicolo dell'interessato	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Trattamento per finalità ulteriori (Whistleblowing)	Dati identificativi	**Base giuridica del trattamento:** adempimento specifiche garanzie di legge per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione (art. 54 – bis del D.lgs. n. 165/2001)
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti (ad es. fiscali, contabili) • Consulenti legali • OIV e Nucleo di Valutazione • Istituti di credito • Amministrazione finanziaria • Compagnie assicurative • Enti pubblici di riferimento • Provider servizi informatici • Unione Comuni del Modenese Area Nord (UCMAN) • Autorità di controllo e giudiziarie • Polo archivistico regionale e archivio comunale	

Commentato [CF8]: Da confermare

Commentato [CF9]: Da confermare

Commentato [CF10]: Da confermare

ORGANIZZAZIONE ENTE (es. Amministratori e Sindaco)	Soggetti che rivestono funzioni di rappresentanza e/o ricoprono cariche istituzionali
I dati sono trasferiti extra UE	No
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto

TERZI/FAMILIARI DIPENDENTE E ORGANI ISTITUZIONALI (compresi amministratori e sindaco)	Soggetti (interessati e no) cui dati sono trattati in quanto in vincoli familiari e di convivenza con il dipendente (interessato) e i membri dell'organizzazione del Titolare	
Tipologie dati trattati	• comuni • particolari (ex artt. 9 e 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • reddituali • contabili e fiscali • relativi allo stato di salute (documentato da certificazioni mediche e nel caso derivati dall'accertamento di una invalidità funzionale) • relativi a condanne penali, reati e a connesse misure di sicurezza	
Finalità necessarie e relative basi giuridiche	Adempimento di specifici obblighi dipendenti, tra l'altro, dalla Legge n. 104/1992 e s.m.i., da decisioni dell'Autorità giudiziaria nei confronti del dipendente in vincolo con l'interessato, o da normative di carattere fiscale e amministrativo di riferimento Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale – AgID	
Trattamento per finalità ulteriori (diffusione)	Dati personali di interesse	**Base giuridica del trattamento:** adempimento obblighi di legge di cui al D.lgs. n. 33/2013
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti (ad es. fiscali, contabili) • Consulenti legali • Enti pubblici di riferimento • Amministrazione finanziaria • Provider servizi informatici • Unione Comuni del Modenese Area Nord (UCMAN) • Polo archivistico regionale e Archivio comunale	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

Commentato [CF11]: Da confermare

FORNITORI	Interessati che offrono o che intendono offrire beni e/o servizi al Titolare	
Tipologie dati trattati	• comuni • particolari (ex art. 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • contabili e fiscali • bancari • curriculari • relativi all'attività commerciale/professionale esercitata • informatici (log di accesso, indirizzo IP, etc.) derivati dalle attività svolte per l'Ente (es. per la gestione delle piattaforme, degli applicativi e/o delle infrastrutture HW e SW di pertinenza dell'Ente anche per le attività di manutenzione degli stessi) e/o dall'uso di piattaforme di pertinenza dell'Ente a cui vengono abilitati i fornitori anche in ragione dell'instaurazione dei rapporti con l'Ente (es. centrali di committenza, mercato elettronico, etc.) • relativi a condanne penali e a reati o alle connesse misure di sicurezza • afferenti alla regolarità contributiva e fiscale	
Finalità necessarie e relative basi giuridiche	Attività di selezione, precontrattuali/contrattuali finalizzati all'instaurazione e erogazione del servizio e/o della fornitura; nonché attività relativa gestione amministrativa e contabile. Adozione provvedimenti amministrativi e gestione relativi procedimenti Adempimento di specifici obblighi in dipendenza delle garanzie in materia di ambiente e sicurezza (es. D.lgs. n. 81/2008) Adempimento degli obblighi di legge conseguenti (es. D.lgs. 50/2016, D.LGS. 36/2023, Legge n. 241/1990, D.P.R. n. 445/2000; Legge n. 190/2012, D.lgs. n. 82/2005, Legge n. 244/ 2007, D.M. n. 55/2013, norme del codice civile laddove applicabili e l'ulteriore normativa pubblicistica, regolamenti comunali di interesse) Gestione del bilancio e della rendicontazione in osservanza della normativa applicabile Gestione del contenzioso Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi e dipendenti dalle attività prestate per l'Ente	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013 Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi) Adempimento degli obblighi dipendenti dalla messa in opera delle banche dati pubbliche

FORNITORI	Interessati che offrono o che intendono offrire beni e/o servizi al Titolare	
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse di cui al fascicolo del contratto/appalto/affidamento	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti (ad es. fiscali, contabili) • Consulenti legali • Nucleo di valutazione- • Enti pubblici di riferimento • Amministrazione finanziaria • Provider servizi informatici • Unione Comuni del Modenese Area Nord (UCMAN) • ANAC • CONSIP e altri mercati elettronici pubblici (es regionali ecc) • Istituti di credito • Imprese concorrenti in caso di esercizio diritto di accesso • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale e archivio comunale • Banche dati pubbliche (es. BDNCP)	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

Commentato [CF12]: Da confermare

Commentato [CF13]: Da confermare

Commentato [CF14]: Da confermar

Commentato [CF15]: Da confermare

VOLONTARI	Interessati i cui dati sono trattati per la gestione del rapportoinstaurato	
Tipologie dati trattati	• comuni • particolari (ex art. 9 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • curriculari • informatici derivati dall'accesso al sito web, alle caselle di posta elettronica, agli applicativi e alle piattaforme di pertinenza dell'Ente e messia disposizione del personale autorizzato ai trattamenti da esso svolti e dipendenti dalle attività svolte • idonei a rivelare lo stato di salute (es. in dipendenza dell'appartenenza alle categorie protette di cui alla Legge n. 68/1999 e s.m.i. o risultanti da certificazioni mediche), o altri dati di natura particolare, anche nel caso questi comunicati per il tramite del curriculum • relativi all'attività prestata	
Finalità necessarie e relative basi giuridiche	Inserimento, nella struttura del Titolare, del candidato risultato idoneo allo svolgimento delle attività in regime volontaristico Adempimento degli obblighi derivanti dal particolare rapporto instaurato e dalla normativa che lo disciplina, tra cui, quelli nei confronti degli istituti di previdenza ed assistenza, sia obbligatorie che integrative Gestione del rapporto instaurato Adozione dei provvedimenti amministrativi e gestione dei relativi procedimenti Adempimento degli obblighi di legge e di regolamento conseguenti (D.lgs.n. 267/2000, Legge n 241/1990, D.P.R. n. 445/2000; Legge n. 64/2001, laddove applicata e applicabile, e leggi regionali di riferimento (es. per l'istituzione dei registri comunali e generali del volontariato) e leggi speciali (bandi di concorso e regolamenti attuativi e/o per l'instaurazione del rapporto), infine regolamenti comunali di interesse Adempimenti obblighi (formativi e/o contabili) dipendenti dal rapporto instaurato Adempimento di specifiche garanzie in materia di ambiente e sicurezza (es. D.lgs. n. 81/2008 Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi e dipendenti dalle attività prestate per l'Ente	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli derivanti dall'iscrizione al registro comunale/generale di volontariato o dall'inserimento negli elenchi dedicati ai progetti di volontariato gestiti dall'Ente

Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo
Destinatari dei dati e/o terzi	• Consulenti legali e in materia contabile e fiscale • Provider servizi informatici • Professionisti in ambito sanitario (D.lgs. n. 81/2008) • RSPP • Enti pubblici di riferimento • Formatori • Unione Comuni del Modenese Area Nord (UCMAN) • Compagnie assicurative in convenzione • Enti convenzionati con cui sussistono accordi in merito alla gestione delle attività di volontariato • Reti di servizi regionali • archivio comunale
I dati sono trasferiti extra UE	No
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto

UTENTI SERVIZI ISTITUZIONALI ANAGRAFE AIRE ELETTORALE STATO CIVILE SERVIZI DEMOGRAFICI E POLIZIA MORTUARIA	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento
Tipologie dati trattati	• comuni • particolari (ex artt. 9 e 10 del GDPR)
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • idonei a rivelare l'origine etnica, l'appartenenza a partiti politici, l'orientamento e la vita sessuale, etc.) e idonei a rivelare lo stato di salute (es. patologie pregresse) • relativi all'attività professionale e lavorativa • relativi alla posizione degli interessati nei confronti del servizio militare e civile • relativi alle candidature a cariche elettive • relativi ai beni e alle proprietà in possesso dell'interessato e censite dal Titolare • relativi alla situazione e alla condizione familiare • relativi a procedimenti giudiziari e a condanne penali e a reati o alle connesse misure di sicurezza • informatici (log di accesso, indirizzo IP, etc.) derivati dall'uso di piattaforme di pertinenza dell'Ente accessibili mediante i siti istituzionali o con l'ausilio di tecnologie messe in opera per la fruizione e la gestione dei servizi esposti in rete (es. Sistema pubblico di identità digitale – SPID, Carta nazionale dei servizi - CNS)
Finalità necessarie e relative basi giuridiche	Adempimento di obblighi previsti da leggi, regolamenti e normativa comunitaria, ovvero in esecuzione di disposizioni impartite da autorità a ciò legittimate e da organi di vigilanza e controllo; in particolare, ed indicativamente, in adempimento della vigente normativa in materia di anagrafe e stato civile, di consultazioni elettorali e referendarie, leva militare e giudici popolari e polizia mortuaria. Adempimento degli obblighi di legge conseguenti. Riguardo alle rispettive materie: D.L. n. 78/2015, convertito, con modificazioni, dalla Legge n. 125/2015 e regolamenti attuativi in materia di emissione della carta di identità elettronica, Legge n. 76/2016, e regolamenti attuativi; D.P.R. n. 126/2015; D.P.C.M. n. 109/2013 e regolamenti attuativi dell'ANPR; D.PC.M. del 10.11.2014 e regolamenti attuativi del Sistema pubblico di identità digitale - SPID; Legge n. 241/1990, Legge n. 190/2012, D.lgs. n. 82/2005 e relative regole tecniche, D.P.R. n. 445/2000, Legge n. 18/1975; Legge n.184/1983 (art.31); D.Lgs. n. 271/1989 (art.39); D.L. n. 223/2006 convertito con Legge n. 248/2006 (art.7); Legge n.183/2011 (art.15); D.M del 12/02/2014); artt. 139 ess. c.p.c. aventi riguardo le notifiche in generale e quelle presso la Casa Comunale

17

Commentato [CF16]: Come indicato nel regolamento sul trattamento dei dati sensibili (confermare)

UTENTI SERVIZI ISTITUZIONALI **ANAGRAFE AIRE ELETTORALE STATO CIVILE SERVIZI DEMOGRAFICI E POLIZIA MORTUARIA**	**Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento**	
	E ancora: D.P.R. n. 939/2000, R. D. n.1238/1939, R.D. n. 262/1942 (titoli VI, VIII, XIV); Legge n. 1064/1955, D.P.R. n. 432/1957; Legge n. 21982012, Legge n. 219/2017; Legge n. 184/1993, Legge n. 91/1992; D.P.R. n. 572/1993, D.P.R. n. 362/1994; Legge n. 379/2000, D.L. 69/2013 convertito dalla Legge n. 98/2013 (art.33); Circolare Ministero dell'Interno del 28.01.1991, Legge n. 847/1929; Legge n. 1159/1929; R.D. n. 289/1930, Leggi regolanti i rapporti con lo Stato e le chiese acattoliche (n.449/1984 – n.516/1988 – n.517/1988 – n.101/1989 – n.116/1995 – n.520/1995 – n.126/2012 – n.127/2012 – n.128/2012 – n.245/2012 – n.246/2012); Legge n. 898/1970, Legge n. 121/1985 (art.8); Legge n. 74/1985 – Legge n. 74/1987 (art.19); D.L. n 132/2014 convertito con Legge n.162/2014, Legge n.55/2015; Legge n. 76/2016, Legge n. 218//1995; E infine, D.P.R. n. 223/1967, D.P.R. n. 313/2002 (art.29); D.P.R. n. 50/1973, D.Lgs. n. 320/1994; D.Lgs. n. 197/1996, Legge n.120/1999 (art.13); D.P.R. n. 299/2000, Legge n. 95/1989; Legge n. 53/1990, Legge n. 15/1991; Legge n. 17/2003, D.L. n. 1/2006 convertito con Legge n. 22/2006 (art.1); Legge n. 81/1993, D.Lgs. n. 267/2000; Legge n. 56/2014, Legge n. 212/1956; Legge n. 515/1993, Legge n. 287/1951; D.P.R. n. 237/1964, Legge n. 191/1975; D.Lgs. n. 504/1997, Legge n. 64/2001; D.Lgs. n. 77/2002, D.M. del 30.12.2003; Legge n. 226/2004, D.P.R. n.169/2005 (art.3) DPR 285/1990 E regolamenti comunali di interesse Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013 Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi)
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico

UTENTI SERVIZI ISTITUZIONALI ANAGRAFE AIRE ELETTORALE STATO CIVILE SERVIZI DEMOGRAFICI E POLIZIA MORTUARIA	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo
Destinatari dei dati e/o terzi	• Enti e organismi pubblici di riferimento • Provider servizi informatici • Organi di pubblica sicurezza • Polo archivistico regionale e archivio comunale • Richiedenti legittimati (es. avvocati) • Banche dati pubbliche (ANPR) • Agenzie onoranze funebri
I dati sono trasferiti extra UE	No tranne AIRE CONSOLATI AMBASCIATE ESTERI di tutto il Mondo previsti e in adempimento normativo in materia e/o salvo quanto previsto in applicazione art. 49 par. 1, lett g del GDPR Regolam. UE 2016/679
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto

19

Commentato [CF17]: Da confermare

UTENTI SERVIZI ISTITUZIONALI LAVORI PUBBLICI	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Tipologie dati trattati	• comuni • particolari (ex artt. 9 e 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • contabili e fiscali • bancari • relativi all'attività professionale e lavorativa prestata • idonei a rivelare lo stato di salute (es. documentati in certificazioni mediche o comunicati in caso di infortunio e di incidenti occorsi in dipendenza dell'esecuzione dei lavori appaltati e/o affidati) • relativi a condanne penali e a reati o alle connesse misure di sicurezza • informatici (log di accesso, indirizzo IP, etc.) derivati dall'uso di piattaforme di negoziazione e di scambio, di pertinenza dell'Ente • relativi alla regolarità contributiva e fiscale	
Finalità necessarie e relative basi giuridiche	Esecuzione e gestione dei rapporti instaurati e delle eventuali misure precontrattuali. Adozione provvedimenti amministrativi e gestione relativi procedimenti Adempimento di specifici obblighi in dipendenza delle garanzie in materia di ambiente e sicurezza (es. D.lgs. n. 81/2008) Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; D.P.R. n. 445/2000; D.lgs. n. 50/2016; Legge n. 190/2012, Legge 241/1990, D.lgs. n. 82/2005 e relative regole tecniche; D.lgs. n. 1/2018, Legge n. 98/2013 e i regolamenti di attuazione del Ministero del Lavoro e delle Politiche sociali; Delibera Cipe del 30 giugno 2014, Legge n. 244/2007 e D.M. n. 55/2013, D.lgs. n. 150/2009; Legge di stabilità 2019; e infine regolamenti comunali di interesse) Gestione del contenzioso (es. risarcimento danni per incidenti, infortuni, etc.) Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013 Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi) Adempimento degli obblighi dipendenti dalla messa in opera delle banche dati pubbliche

20

Commentato [CF18]: Da confermare

UTENTI SERVIZI ISTITUZIONALI LAVORI PUBBLICI	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti legali e fiscali • Enti e organismi pubblici di riferimento • Amministrazione finanziaria e catastale e demaniale • AUSL e professionisti del settore sanitario • Compagnie assicuratrici • Istituti di credito • Amministrazioni condominiali • Imprese concorrenti nell'esercizio del diritto di accesso • Società di gestione del patrimonio • Provider servizi informatici • ANAC • ARPAE • ATERSIR • CONSIP • OIV e Nucleo di Valutazione • Centrale unica di committenza (CUC) della Provincia di Modena • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale e archivio comunale • Banche dati pubbliche (es. BDNCP e BDAP)	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

21

Commentato [CF19]:

Commentato [20]:

Commentato [CF21]:

Commentato [CF22]:

Commentato [CF23]: Da confermare

Commentato [CF24]: e

Commentato [CF25]:

UTENTI SERVIZI ISTITUZIONALI URBANISTICA ED EDILIZIA PRIVATA	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Tipologie dati trattati	• comuni • particolari (ex artt. 9 e 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • contabili e fiscali • bancari • relativi ai titoli edilizi e al patrimonio privato • relativi all'attività professionale e lavorativa prestata • idonei a rivelare lo stato di salute (es. documentati in certificazioni mediche nel caso per esempio di richieste per la rimozione di barriere architettoniche) • relativi a procedimenti sanzionatori, a condanne penali e a reati o alle connesse misure di sicurezza • informatici (log di accesso, indirizzo IP, etc.) derivati dall'uso di piattaforme di pertinenza dell'Ente accessibili anche mediante il Sistema pubblico di identità digitale - SPID o la Carta nazionale dei servizi - CNS	
Finalità necessarie e relative basi giuridiche	Esecuzione e gestione delle attività di controllo, indirizzo e presidio Adozione provvedimenti autorizzativi e sanzionatori e gestione relativi procedimenti Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; D.P.R. n. 445/2000; D.P.R. n. 380/2001; Legge n. 241/1990, Legge n. 13/1989 e relativi regolamenti attuativi; Legge n. 229/2016; D.lgs. n. 1/2018; D.lgs. n. 50/2016; Legge n. 190/2012, Legge 241/1990, D.lgs. n. 42/2004, D.lgs. n. 82/2005 e relative regole tecniche; D.PC.M. del 10.11.2014 e regolamenti attuativi del Sistema pubblico di identità digitale – SPID; articoli 1175, 1227, 1375 del codice civile; D.lgs. n. 150/2009; regolamenti edilizi e piani regolatori e altri regolamenti comunali di interesse) Gestione del bilancio e della rendicontazione in osservanza della normativa applicabile Gestione del contenzioso Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013 Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi)

Commentato [CF26]: e

22

Commentato [CF27]: Da confermare

UTENTI SERVIZI ISTITUZIONALI URBANISTICA ED EDILIZIA PRIVATA	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti legali e tecnici • Enti e organismi pubblici di riferimento • Istituti di credito • Amministrazione finanziaria e del territorio • Società di gestione dei servizi e delle certificazioni (es. SOA) • Consorzi di bonifica • Provider servizi informatici • OIV • Unione Comuni del Modenese Area Nord (UCMAN) • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale e archivio comunale • Richiedenti legittimati (es rappresentanti/delegati dell'interessato)	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

Commentato [CF26]: e

23

Commentato [CF28]:

UTENTI SERVIZI ISTITUZIONALI CONTRATTI, GARE E APPALTI	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Tipologie dati trattati	• comuni • particolari (ex art. 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • contabili e fiscali • bancari • relativi all'attività professionale e lavorativa prestata • relativi a condanne penali e a reati o alle connesse misure di sicurezza • informatici (log di accesso, indirizzo IP, etc.) derivati dall'uso di piattaforme di negoziazione e di scambio, di pertinenza dell'Ente	
Finalità necessarie e relative basi giuridiche	Esecuzione e gestione dei rapporti instaurati e delle eventuali misure precontrattuali. Adempimento di specifici obblighi in dipendenza delle garanzie in materia di ambiente e sicurezza (es. D.lgs. n. 81/2008) Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; D.lgs. n. 50/2016; Legge n. 190/2012, Legge 241/1990, D.lgs. n. 82/2005 e relative regole tecniche; Legge n. 98/2013 e i regolamenti di attuazione del Ministero del Lavoro e delle Politiche sociali; Delibera Cipe del 30 giugno 2014, Legge n. 244/2007 e D.M. n. 55/2013, D.lgs. n. 150/2009 e infine regolamenti comunali di interesse), D.LGS. 36/2023 Gestione del bilancio e della rendicontazione in osservanza della normativa applicabile Gestione del contenzioso Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013 Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi) Adempimento degli obblighi dipendenti dalla messa in opera delle banche dati pubbliche

24

Commentato [CF29]:

UTENTI SERVIZI ISTITUZIONALI CONTRATTI, GARE E APPALTI	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti legali e fiscali • Enti e organismi pubblici di riferimento • Amministrazione finanziaria • Istituti di credito • Imprese concorrenti nell'esercizio del diritto di accesso • Provider servizi informatici • ANAC • CONSIP • Altri mercati elettronici della pubblica amministrazione (regionali, ecc) • Nucleo di Valutazione • Centrale unica di committenza (CUC) della Provincia di Modena • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale e archivio comunale • Banche dati pubbliche (es. BDNCP)	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

25

Commentato [CF30]:

Commentato [CF31]:

Commentato [32]:

Commentato [CF33]:

UTENTI SERVIZI ISTITUZIONALI MANUTENZIONI	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Tipologie dati trattati	• comuni • particolari (ex artt. 9 e 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • economici e amministrativi • idonei a rivelare lo stato di salute (es. documentazione attestante incidenti e infortuni occorsi all'utenza e/o al personale del fornitore) • relativi all'attività professionale e lavorativa prestata • relativi a condanne penali e a reati o alle connesse misure di sicurezza	
Finalità necessarie e relative basi giuridiche	Esecuzione e gestione delle attività di ripristino e messa in sicurezza edifici, luoghi pubblici e fornitura dei relativi servizi manutentivi Gestione delle segnalazioni degli utenti Adozione provvedimenti conseguenti e gestione relativi procedimenti Adempimento di specifici obblighi in dipendenza delle garanzie in materia di ambiente e sicurezza (es. D.lgs. n. 81/2008) Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; D.lgs. n. 50/2016; Legge n. 190/2012, Legge 241/1990, D.lgs. n. 82/2005 e relative regole tecniche; D.P.R. n. 445/2000; e infine regolamenti comunali di interesse) Gestione del bilancio e della rendicontazione in osservanza della normativa applicabile Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013 Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi) Adempimento degli obblighi dipendenti dalla messa in opera delle banche dati pubbliche

UTENTI SERVIZI ISTITUZIONALI MANUTENZIONI	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse (relativi ai report delle segnalazioni degli utenti)	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Fornitori servizi tecnici • Enti e organismi pubblici di riferimento • Amministrazione finanziaria • CONSIP • Provider servizi informatici • Centrale unica di committenza (CUC) della Provincia di Modena • Unione Comuni del Modenese Area Nord (UCMAN) • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale e archivio comunale • Banche dati pubbliche (es. BDNCP)	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

27

Commentato [CF34]:

Commentato [CF35]:

Commentato [CF36]:

Commentato [CF37]:

UTENTI SERVIZI ISTITUZIONALI SERVIZI ALLA PERSONA (CULTURA, SPORT CACCIA PESCA ASSOCIAZIONISMO)	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Tipologie dati trattati	• comuni • particolari (ex art. 9 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • idonei a rivelare lo stato di salute (es. mediante certificazioni mediche) • informatici (log di accesso, indirizzo IP, etc.) derivati dall'uso di piattaforme di pertinenza dell'Ente accessibili anche mediante il Sistema pubblico di identità digitale – SPID o la Carta nazionale dei servizi - CNS per la fruizione dei servizi comunali esposti in rete	
Finalità necessarie e relative basi giuridiche	Esecuzione e gestione dei servizi erogati, controllo e monitoraggio della loro regolare fruizione Adozione provvedimenti autorizzativi/amministrativi e gestione relativi procedimenti Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; Legge 241/1990, D.lgs. n. 82/2005 e relative regole tecniche; D.PC.M. del 10.11.2014 e regolamenti attuativi del Sistema pubblico di identità digitale – SPID; D.P.R. n. 445/2000; D.LGS. 117/2017, normativa regionale in materia e infine regolamenti comunali di interesse Gestione del bilancio e della rendicontazione in osservanza della normativa applicabile Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013 Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi)
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico

28

Commentato [CF38]:

UTENTI SERVIZI ISTITUZIONALI SERVIZI ALLA PERSONA (CULTURA, SPORT CACCIA PESCA ASSOCIAZIONISMO)	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Trattamento per finalità ulteriori (promozione eventi culturali e sociali)	Dati personali identificativi e di contatto	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Trattamenti per finalità ulteriori (invio newsletter)	Dati personali identificativi e di contatto	**Base giuridica del trattamento:** consenso e/o esecuzione di compiti di interesse pubblico
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti del settore • Enti e organismi pubblici di riferimento • Associazioni di volontariato ed enti del terzo settore di cui al D.LGS 117/2017 in generale • Associazioni sportive e culturali • OIV e Nucleo di Valutazione • Amministrazione finanziaria • Provider servizi informatici • Unione Comuni del Modenese Area Nord (UCMAN) • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale e archivio comunale • Sistemi bibliotecari regionali e nazionali • Registro unico nazionale enti terzo settore (RUNTS) • Richiedenti legittimati (rappresentanti, delegati dell'interessato)	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

29

Commentato [CF39]:

Commentato [CF40]:

Commentato [CF41]:

Commentato [42]:

UTENTI SERVIZI ISTITUZIONALI SERVIZI ALLE IMPRESE (COMMERCIO E ATTIVITA' PRODUTTIVE PROMOZIONE DEL TERRITORIO)	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
Tipologie dati trattati	• comuni • particolari (ex art. 10 del GDPR)	
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • bancari • economici, contabili e fiscali • relativi all'attività professionale e commerciale prestata • relativi a condanne penali/reati e a connesse misure di sicurezza • informatici (log di accesso, indirizzo IP, etc.) derivati dall'uso di piattaforme di pertinenza dell'Ente accessibili anche mediante il Sistema pubblico di identità digitale – SPID o la carta nazionale dei servizi - CNS, per la fruizione dei servizi comunali esposti in rete (es. Sportello Unico telematico attività produttive - SUAP)	
Finalità necessarie e relative basi giuridiche	Esecuzione e gestione delle attività istituzionali di interesse, quali, tra le altre: il rilascio licenze commerciali, nulla osta, permessi e autorizzazioni; l'erogazione di contributi e finanziamenti Adozione relativi provvedimenti amministrativi e nel caso sanzionatori Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; Legge 241/1990, D.lgs. n. 82/2005 e relative regole tecniche; D.P.C.M. del 10.11.2014 e regolamenti attuativi del Sistema pubblico di identità digitale - SPID; D.P.R. n. 445/2000; D.lgs. n. 222/2016; D.lgs. n. 160/2010; D.lgs. n. 59/2010; e infine regolamenti comunali di interesse Gestione del bilancio e della rendicontazione in osservanza della normativa applicabile Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013 Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi)

30

Commentato [CF43]:

Commentato [CF44]:

UTENTI SERVIZI ISTITUZIONALI SERVIZI ALLE IMPRESE (COMMERCIO E ATTIVITA' PRODUTTIVE PROMOZIONE DEL TERRITORIO)	**Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento**	
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti legali e fiscali • Consulenti di settore e tecnici • Enti e organismi pubblici di riferimento • AUSL • OIV e Nucleo di Valutazione • Amministrazione finanziaria e doganale • CCIAA • ANAC • ARPAE • Società partecipate/controllate per la gestione dei servizi • Provider servizi informatici • Unione Comuni del Modenese Area Nord (UCMAN) • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale e archivio comunale • Banche dati pubbliche (BDNA) e archivio comunale • Rappresentanti/delegati dell'interessato	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

Commentato [CF45]:

Commentato [CF46]:

Commentato [CF47]:

Commentato [CF48]:

TERZI/FAMILIARI/ CONVIVENTI/RAPPRESENTANTI/ EREDI/ASSOCIAZIONI PROFESSIONALI/DELEGATI UTENTI SERVIZI ISTITUZIONALI (ES. SERVIZI ALLA PERSONA, COMMERCIO, LAVORI PUBBLICI, MANUNTENZIONE, AMBIENTE, EDILIZIA E URBANISTICA, ANAGRAFE E SERVIZI DEMOGRAFICI POLIZIA MORTUARIA)	**Soggetti (interessati e no) che rappresentano, sono delegati o in vincolo anche familiare con gli utenti (interessati)**
Tipologie dati trattati	• comuni • particolari (ex art. 9 e 10 del GDPR)
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • bancari • contabili e fiscali • relativi all'attività professionale e commerciale prestata • relativi a condanne penali, reati e a connesse misure di sicurezza • idonei a rivelare lo stato di salute (documentato per esempio attraverso certificazioni mediche attestanti altresì invalidità funzionale) e altri dati particolari (origine etnica, razziale, credo religioso etc.) • informatici (log di accesso, indirizzo IP, etc.) derivati dall'uso di piattaforme di pertinenza dell'Ente accessibili anche mediante il Sistema pubblico di identità digitale – SPID o la carta nazionale dei servizi - CNS, per la fruizione dei servizi comunali esposti in rete (es. ANPR o SUAP, SUE e pagamenti elettronici)
Finalità necessarie e relative basi giuridiche	Esecuzione e gestione delle attività istituzionali di interesse Adozione relativi provvedimenti amministrativi e gestione procedimenti presupposti e conseguenti Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; Legge 241/1990, D.lgs. n. 82/2005 e relative regole tecniche; D.PC.M. del 10.11.2014 e regolamenti attuativi del Sistema pubblico di identità digitale – SPID; D.P.R. n. 445/2000; R.D. n. 1265/1934, R.D. n. 1379/1937; D.P.R. n. 285/1990; Legge n. 578/1993; D.M. n. 582/1994, Legge n. 130/2001; D.P.R. n. 254/2003, D.M. del 11.04.2008; leggi regionali di interesse e delibere di giunta; Circolare ministero sanità n.24/1993; la normativa applicata ai diversi settori a cui accede il terzo per conto dell'utente; infine regolamenti comunali di interesse Gestione del bilancio e della rendicontazione in osservanza della normativa applicabile Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti

32

Commentato [CF49]:

Commentato [CF50]:

Commentato [51]:

Commentato [CF52]:

TERZI/FAMILIARI/ CONVIVENTI/RAPPRESENTANTI/ EREDI/ASSOCIAZIONI PROFESSIONALI/DELEGATI UTENTI SERVIZI ISTITUZIONALI (ES. SERVIZI ALLA PERSONA, COMMERCIO, LAVORI PUBBLICI, MANUNTENZIONE, AMBIENTE, EDILIZIA E URBANISTICA, ANAGRAFE E SERVIZI DEMOGRAFICI POLIZIA MORTUARIA)	**Soggetti (interessati e no) che rappresentano, sono delegati o in vincolo anche familiare con gli utenti (interessati)**	
	altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento:** adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse	**Base giuridica del trattamento:** esecuzione di compiti di interesse pubblico
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti e professionisti di vario genere • Enti e organismi pubblici di riferimento • AUSL • Istituti di credito • Amministrazione finanziaria • Provider servizi informatici • Unione Comuni del Modenese Area Nord (UCMAN) • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale e archivio comunale **N.B.:** per destinatari vanno intesi, nel caso anche quelli di cui alle tabelle precedenti allorchè il terzo faccia accesso per conto dell'utente ai servizi ivi descritti	
I dati sono trasferiti extra UE	No	
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto	

Commentato [CF53]: Da confermare

Commentato [CF54]:

UTENTI SITO WEB	Interessati che accedono al sito web istituzionale e ai servizi offerti per il loro tramite
Tipologie dati trattati	• comuni
Dati trattati	• identificativi, di recapito e di contatto • informatici (log di accesso, indirizzo IP, etc.) derivati dall'uso di piattaforme di pertinenza dell'Ente e accessibili tramite il sito web istituzionali e comunque quelli raccolti mediante: • cookie tecnici e di funzionalità • cookie di analisi
Finalità necessarie e relative basi giuridiche	Accesso ai servizi esposti in rete, alle informazioni circa le attività amministrative, deliberative e istituzionali dell'Ente, in adempimento degli obblighi al fine facenti capo al Titolare (es. D.lgs. n. 82/2005, D.lgs. n. 33/2013, Legge n. 69/2009, regolamenti comunali di interesse) Adempimento di ulteriori obblighi di legge, quali quelli aventi riguardo all'accessibilità ai siti web delle pubbliche amministrazioni di cui alla legge n. 4/2004 e al D.lgs. n. 106/2018 Per i - cookie tecnici e di funzionalità: ne viene fatto uso per quanto strettamente necessario al funzionamento e all'esplorazione sicura ed efficiente del sito web e per facilitare la navigazione e il servizio reso all'utente in funzione di una serie di criteri da quest'ultimo selezionati - i cookie di analisi: ne viene fatto uso per quanto strettamente necessario a raccogliere informazioni in forma aggregata sulla navigazione da parte degli utenti per ottimizzare l'esperienza di navigazione e i servizi accessibili mediante il sito e per consentire l'utilizzo di funzioni come il benchmarking e la pubblicazione e che consentono di verificare le visite al sito Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID
Scelte automatizzate prese sull'interessato utilizzando i dati trattati	Nessuna
Modalità di trattamento	Dati trattati in formato elettronico
Destinatari dei dati e/o terzi	• Provider servizi informatici • Terze parti (per i cookie) • Unione Comuni del Modenese Area Nord (UCMAN) • Agenzia per l'Italia digitale (AgID) – Difensore civico per il digitale • Autorità di controllo e giudiziarie competenti • Sistemi informatici in connessione applicativa
Siti web che trattano dati degli interessati	• https://www.comune.medolla.mo.it/
I dati sono trasferiti extra UE	No

Commentato [CF55]:

34

Commentato [CF56]:

UTENTI SITO WEB	Interessati che accedono al sito web istituzionale e ai servizi offerti per il loro tramite
Data retention	Si veda la versione corrente del Piano di data retention richiamato e, per i trattamenti che vi sono sottoposti, il DPIA corrispondente.

Commentato [CF55]:

Commentato [CF57]:

AMMINISTRATORI DI SISTEMA (ADS)	Soggetti che , muniti di specifico incarico, svolgono le funzioni di amministrazione dei sistemi in uso presso il Titolare
Tipologie dati trattati	• comuni
Dati trattati	• identificativi, quali tra gli altri quelli funzionali all'autenticazione informatica e alla gestione dei privilegi di accesso dell'ADS • log di accesso alle risorse informatiche in uso dall'Ente • relativi all'attività di manutenzione e assistenza sulle risorse a cui l'ADS è associato in base ai privilegi ricevuti
Finalità necessarie e relative basi giuridiche	Registrazione accessi logici dell'ADS ai sistemi in uso presso il titolare al fine verificarne l'operato ai sensi per gli effetti del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, pro – tempore vigente Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, dalle linee guida dell'Agenzia per l'Italia digitale - AgID
Modalità di trattamento	Dati trattati in formato elettronico
Destinatari dei dati e/o terzi	• Autorità di pubblica sicurezza
I dati sono trasferiti extra UE	No
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto

Commentato [CF58]:

VISITATORI	Interessati che accedono ai locali del Titolare
Tipologie dati trattati	• comuni
Dati trattati	• identificativi, anagrafici, di recapito e di contatto
Finalità necessarie e relative basi giuridiche	Gestione utenza
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo
Destinatari dei dati e/o terzi	• Autorità competenti • Fornitori allo scopo individuati
I dati sono trasferiti extra UE	No
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto

SERVIZI DI CONTROLLO TECNOLOGICO DEL TERRITORIO (VIDEOSORVEGLIANZA)	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento
Tipologie dati trattati	• Comuni • particolari (ex artt. 9 e 10 del GDPR)
Dati trattati	• immagini rilevate mediante gli impianti di videosorveglianza dislocati sul territorio di interesse e dai sistemi di videosorveglianza in mobilità (Bodycam)
Finalità necessarie e relative basi giuridiche	Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito l'Ente Attività di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica Attività di rilevazione infrazioni a norme di legge o regolamento, di competenza specifica della Polizia locale e di controllo del territorio (attività diverse e distinte da quelle precedenti) Adozione provvedimenti amministrativi e sanzionatori e gestione relativi procedimenti Adempimento degli obblighi conseguenti alle convenzioni stipulate tra l'Ente e l'Unione Comuni Modenesi Area Nord (UCMAN), per la gestione associata e coordinata del servizio di polizia amministrativa locale (conv. rep. n. 13/2004, conv. rep. n. 232/2006, conv. rep. n. 382/2008, conv. rep. n. 577/2010, conv. rep. n. 807/2017, e s.m.i.) Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; Legge 241/1990, D.lgs. n. 82/2005 e relative regole tecniche; D.P.R. n. 445/2000; Legge n. 65/1986; Legge-quadro sull'ordinamento della polizia municipale; D.lgs. n. 51/2018; Legge n. 48/2017, Linee generali delle politiche pubbliche per la sicurezza urbana integrata; Legge n. 689/1981, D.lgs. n. 285/1992; Norme penali di rilievo, leggi regionali, delibere consiliari e di giunta e regolamenti comunali di interesse Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, alle linee guida dell'Agenzia per l'Italia digitale – AgID Adempimento delle prescrizioni, anche di ordine tecnico-organizzativo, derivanti da: - i patti per l'attuazione della sicurezza urbana e installazione di sistemi di videosorveglianza - il regolamento di polizia urbana - il disciplinare interno sull'uso dei sistemi di videosorveglianza, compresi quelli in mobilità (bodycam) - i provvedimenti dell'Autorità garante in materia di videosorveglianza e di trattamenti svolti mediante sistemi di videosorveglianza in mobilità - la Legge n. 300/1970

SERVIZI DI CONTROLLO TECNOLOGICO DEL TERRITORIO (VIDEOSORVEGLIANZA)	Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento	
	Adempimento delle misure tecnico/organizzative stabilite a seguito della valutazione di impatto privacy nel caso effettuata alle condizioni e secondo le modalità di cui all'articolo 35 del GDPR	
Trattamento dati per finalità ulteriori (interconnessione)	Dati identificativi di interesse	**Base giuridica del trattamento: adempimento ed esecuzione di compiti di interesse pubblico anche in specie derivati dalla concreta attuazione della Legge n. 48/2017**
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti legali, tecnici, della procura e ausiliari di polizia giudiziaria • Enti e organismi pubblici di riferimento (es. Prefettura, PRA, Motorizzazione civile, Regione e Provincia) • Altre forze di polizia • OIV • Provider servizi informatici • Unione Comuni Modenesi Area Nord (UCMAN) • Autorità di controllo e giudiziarie competenti	
I dati sono trasferiti extra UE	No	
Data retention	Le immagini sono conservate, , nel perseguimento delle finalità di sicurezza urbana, per un tempo non superiore a 98 (novantotto) ore, ossia fino a 7 (sette) giorni, dalla loro registrazione, con sovraregistrazione al termine, fatte salve esigenze di ulteriore conservazione nel caso in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria o all'eventuale esercizio del diritto di accesso riconosciuto all'interessato in virtù degli art. 15 e ss, del GDPR o da quello di cui agli artt. 22 e ss. della legge n. 241/1990	

UTENTI (es. richiedenti, trasgressori, sanzionati, danneggiati, controparti, periti e rappresentanti) SERVIZI ISTITUZIONALI **SERVIZI PRESTATI DALLA POLIZIA MUNICIPALE DELL'UNIONE**	**Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento**
Tipologie dati trattati	• comuni • particolari (ex artt. 9 e 10 del GDPR)
Dati trattati	• identificativi, anagrafici, di recapito e di contatto • relativi alla situazione reddituale, economica e familiare • idonei a rivelare lo stato di salute (es. documentati in certificazioni mediche e in quelle attestanti invalidità funzionale e disabilità) e altri dati particolari (quali quelli relativi all'origine razziale e etnica e al credo religioso, etc.) • relativi all'attività professionale e commerciale prestata • relativi a condanne penali/reati e a connesse misure di sicurezza • informatici (log di accesso, indirizzo IP, indirizzi di posta elettronica, etc.) derivati anche dall'uso di piattaforme di pertinenza dell'Ente accessibili anche mediante il Sistema pubblico di identità digitale – SPID o la Carta nazionale dei servizi - CNS per la fruizione dei servizi esposti in rete
Finalità necessarie e relative basi giuridiche	Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito l'Ente Adozione provvedimenti autorizzativi/amministrativi e sanzionatori e gestione relativi procedimenti Attività di prevenzione, indagine, accertamento e perseguimento di reati, o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica Adempimento degli obblighi conseguenti alle convenzioni stipulate tra l'Ente e l'Unione Comuni Modenesi Area Nord (UCMAN), per la gestione associata e coordinata del servizio di polizia amministrativa locale (conv. rep. n. 13/2004, conv. rep. n. 232/2006, conv. rep. n. 382/2008, conv. rep. n. 577/2010, conv. rep. n. 807/2017, e s.m.i.) Adempimento degli obblighi di legge conseguenti (ex multis, D.lgs. n. 267/2000; Legge 241/1990, D.lgs. n. 82/2005 e relative regole tecniche; D.PC.M. del 10.11.2014 e regolamenti attuativi del Sistema pubblico di identità digitale – SPID; D.P.R. n. 445/2000; Legge n. 65/1986; Legge-quadro sull'ordinamento della polizia municipale; D.lgs. n. 151/2012, D.lgs. n. 285/1992; Legge n. 689/1981, Legge n. 833/1978; Legge n. 38/2009, D.lgs. n. 222/2016; D.lgs. n. 51/2018; Legge n. 48/2017, Linee generali delle politiche pubbliche per la sicurezza urbana integrata; Norme penali di

UTENTI (es. richiedenti, trasgressori, sanzionati, danneggiati, controparti, periti e rappresentanti) SERVIZI ISTITUZIONALI **SERVIZI PRESTATI DALLA POLIZIA MUNICIPALE DELL'UNIONE**	**Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento**	
	rilievo, leggi regionali, delibere consiliari e di giunta e regolamenti comunali di interesse Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR) e dipendenti altresì dalla normativa tecnica e regolamentare anche di derivazione ministeriale e, altresì, alle linee guida dell'Agenzia per l'Italia digitale - AgID	
Trattamento dati per finalità ulteriori (diffusione)	Dati personali identificativi sottoposti a pubblicazione	**Base giuridica del trattamento: adempimento di specifici obblighi di legge e in particolare di quelli di cui al D.lgs. n. 33/2013** **Adempimento di specifici obblighi di legge aventi riguardo la pubblicità legale mediante albo pretorio on line (Legge n. 69/2009 e relativi regolamenti attuativi)**
Trattamento per finalità ulteriori (archiviazione per interesse pubblico e per scopi statistici)	Dati personali di interesse	**Base giuridica del trattamento: esecuzione di compiti di interesse pubblico**
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo	
Destinatari dei dati e/o terzi	• Consulenti legali, tecnici e della procura di competenza e ausiliari di polizia giudiziaria • Enti e organismi pubblici di riferimento (es. Prefettura, PRA, Motorizzazione civile, Regione e Provincia) • AUSL • Altre forze di polizia • Amministrazione finanziaria • Fornitori servizi accessori (es. postalizzazione) • OIV o nucleo di valutazione • Provider servizi informatici • Unione Comuni Modenesi Area Nord (UCMAN) • Autorità di controllo e giudiziarie competenti • Polo archivistico regionale o Archivio comunale di deposito in base a convenzione	
I dati sono trasferiti extra UE	No	

UTENTI (es. richiedenti, trasgressori, sanzionati, danneggiati, controparti, periti e rappresentanti) **SERVIZI ISTITUZIONALI** **SERVIZI PRESTATI DALLA POLIZIA MUNICIPALE DELL'UNIONE**	**Interessati che fruiscono dei servizi del Titolare gestiti dall'area/ufficio di riferimento**
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto

TRATTAMENTO MEDIANTE REGISTRAZIONI AUDIO VIDEO E FOTOGRAFICHE	Interessati (compresi i dipendenti, Sindaco, Assessori e Consiglieri) che partecipano agli eventi organizzati dall'Ente comprese sedute consiliari o altri incontri istituzionali
Tipologie dati trattati	• comuni
Dati trattati	• dati identificativi, anagrafici, di recapito e di contatto; • immagini video e foto riconducibili agli interessati
Finalità necessarie e relative basi giuridiche	Esecuzione di compiti istituzionali di documentazione e pubblicità degli eventi e dell'attività del Titolare Regolamento Comunale per le riprese e diffusione in diretta o differita streaming via web delle sedute del consiglio comunale DCC 33 del 10/6/2023 Finialità di comunicazione e informazione del Comune ai sensi L. 150 del 7/6/2000 "Disciplina delle attività di informazione e comunicazione delle pubbliche amministrazioni" e relativi regolamenti attuativi DPR 21/9/2001 N. 422, Direttiva 7/2/2002 "attività di comunicazione delle pubbliche amministrazioni" Autorizzazione rilasciata per l'uso delle immagini ai sensi degli artt. 10 e 320del Codice Civile e degli artt. 96 e 97 della Legge del 22 aprile 1941, n. 633 (Legge sul diritto d'autore) Adempimento delle attività funzionali al trattamento principale, quali quelle finalizzate alla divulgazione dell'evento, e alla archiviazione e alla riproduzione in remoto dell'evento Messa in opera delle misure atte a garantire la sicurezza e la capacità diuna rete o dei server ad essa connessi di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano ladisponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi Adempimento di obblighi di legge (rilevazione e notificazione di eventi di personal data breach ex art. 33 del GDPR)
Consenso	Consenso qualora necessario oppure non necessario per finalità istituzionali consiglio comunale Autorizzazione rilasciata per l'uso delle immagini ai sensi degli artt. 10 e 320 del Codice Civile e degli artt. 96 e 97 della Legge del 22 aprile 1941, n. 633(Legge sul diritto d'autore)
Modalità di trattamento	Dati trattati sia in formato elettronico che in formato cartaceo
Destinatari dei dati e/o terzi	• i professionist, i addetti alle riprese e alla loro riproduzione operatori fotografi, montatori professionali, etc.) • agenzie di stampa • provider di servizi grafici e/o tipografici, di web marketing e/o di editoria multimediale • provider dei servizi informatici • Polo archivistico regionale e archivio comunale • Ditta incaricata sbobinatura audio-video delle sedute di consiglio comunale • Unione Comuni del Modenese Area Nord (UCMAN)

Commentato [MP59]:

I dati sono trasferiti extra UE	No
Data retention	Si veda la versione corrente del Piano di data retention/conservazione e scarto

RIFERIMENTI DOCUMENTALI

- **Nomine per i soggetti autorizzati al trattamento**
- **Nomine per i responsabili del trattamento**
- **Piano di data retention**
- **Incarico al Data Protection Officer**

4. Sistemi Informativi

Commentato [CF60]: i

44

4.1 *Approccio basato sul rischio*

Nella scelta di adeguate misure tecniche rispetto ai trattamenti effettuati, il Titolare ove necessario deve adottare misure che siano costantemente monitorate ed aggiornate.

A tal scopo, il Titolare ha approcciato la materia della *data protection* basandosi su una valutazione preventiva dei rischi effettuata attraverso un vulnerability assessment che ha tenuto conto:

- del contesto di riferimento;
- delle attività di trattamento;
- delle tipologie di dati trattati e del relativo flusso;
- degli strumenti tecnologici utilizzati per il trattamento;
- delle misure di sicurezza già implementate e in corso di implementazione,

così da valutare gli impatti sulla violazione dei diritti e delle libertà degli interessati, e preservare i dati dalla perdita, distruzione o trattamenti non conformi.

A seguito dei risultati del vulnerability assessment, il Titolare ha predisposto un piano migliorativo deputato a pianificare - anche nel tempo - interventi volti ad innalzare il livello di protezione dei dati, calmierando il rischio, e fornendo quindi una migliore tutela degli interessati.

Le implementazioni sono state decise secondo un ordine di priorità che si è basato sia sui livelli di rischio emersi a seguito della valutazione sia sulla realizzabilità tecnica dell'upgrade, ed ha coinvolto figure interne e fornitori esterni ritenuti idonei a fornire un congruo supporto nelle nuove implementazioni.

Il Titolare effettua con cadenza regolare i *vulnerability assessment* per tenere monitorati i livelli di rischio.

4.2 *Applicativi: Privacy by Design e Privacy by Default*

Un tema di particolare rilevanza affrontato dal Titolare nell'ambito della *compliance* al GDPR riguarda altresì gli aspetti tecnici, documentali e procedurali che interessano gli applicativi (software, pacchetti di software, sistemi, app, ecc.), utilizzati per il trattamento dei dati personali.

Il Titolare ha, pertanto, effettuato una mappatura degli applicativi utilizzati, successivamente classificandoli in base ai rischi derivanti ai diritti e alle libertà degli interessati, avuto riguardo alle categorie di interessati ed ai trattamenti effettuati attraverso tali strumenti.

Tale classificazione è stata effettuata secondo i seguenti criteri:

Applicativi	Criteri di rischio
analizzati in dettaglio rispetto ai principi di privacy by design/default	Effettuano trattamenti massivi di dati; Effettuano trattamenti particolari di dati; [alternativi o congiunti]
analizzati solo lato sicurezza e data retention	Non effettuano trattamenti massivi di dati; Non effettuano trattamenti particolari di dati; [alternativi o congiunti]

Applicativi	Criteri di rischio
esclusi dall'analisi di privacy by design/default	Non effettuano trattamenti di dati personali

Con particolare riferimento agli applicativi di cui alla prima sezione della tabella sustante, questi sono stati singolarmente esaminati mediante una *gap analysis* dedicata e fondata sui principi che compongono la privacy by design. In particolare:

I. Approccio proattivo non reattivo, prevenire per correggere: ossia anticipare e prevenire gli eventi invasivi/lesivi della privacy prima che essi accadano;

II. Privacy come impostazione di default: realizzare il massimo livello di privacy, assicurando che i dati personali sono automaticamente protetti in un qualunque sistema IT;

III. Privacy assimilata alla progettazione;

IV. Sicurezza dell'intero ciclo-vita di un sistema e dei dati;

V. Visibilità e trasparenza costante verso l'interessato/utente e centralità dell'utente.

4.3 *Misure di Sicurezza*

In relazione agli aspetti inerenti la sicurezza informatica, sussiste alla data odierna un sistema di misure tecniche efficaci a garantire un livello di sicurezza adeguato al rischio, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento dei dati personali.

Misure di Sicurezza	Misura Adottata? SI/NO/ PARZIALE	Misura da Adottare? SI/NO	Specifiche
Sistemi Antintrusione	SI		
Sistema di guardiania e sorveglianza	NO		Sussistono le telecamere di videosorveglianza sui tre ingressi principali dei quali normalmente (salvo casi eccezionali) solo uno è adibito ad ingresso del pubblico e dei dipendenti. Le immagini di tali telecamere sono visibili dalla Polizia Locale dell'Unione solo Presidio di Medolla.
Videosorveglianza Perimetrale	parziale		
Controllo Accessi	NO		Sussistono le telecamere di videosorveglianza sui tre ingressi principali dei quali normalmente (salvo casi eccezionali) solo uno è adibito ad ingresso del pubblico e dei dipendenti. Le immagini di tali telecamere sono visibili dalla Polizia Locale dell'Unione solo Presidio di Medolla.

Misure di Sicurezza	Misura Adottata? SI/NO/ PARZIALE	Misura da Adottare? SI/NO	Specifiche
Armadi con serratura	PARZIALE		Armadi con serratura tranne qualche eccezione
Locali chiusi a chiave	SI		
Sistema Antincendio	SI		
Sensibilizzazione e Formazione del Personale	PARZIALE		
Copia degli archivi	Parziale		
Backup	Si		Il backup viene garantito sui sistemi server. I dipendenti sono tenuti ad archiviare le informazioni sui server e non sulle postazioni client come indicato nel regolamento di utilizzo delle postazioni Informatiche
Sistemi di Autenticazione Informatica	si		Il sistema si basa su domani controller Active directory ed OpenLdap
Sistemi di Autorizzazione Informatica	si		Il sistema di autorizzazione e' gestito a livello di Dominio per quanto attiene all'accesso al File server; a livello applicativo per quanto attiene all'utilizzo degli applicativi informatici in dotazione agli enti
Soluzioni di Intrusion Detection	no	no	
Firewall	si		La rete di ogni ente e' dotata di sistemi difirewalling perimetrali per l'accesso a internet ed alle varie DMZ o RPV. E' inoltre presente un firewall centralizzato per l'accesso dei client a internet
Rete Privata Virtuale (Intranet)	si		I sistemi dei comuni aderenti all'UCMAN sono interconnessi attraverso una RPV L3 gestita da Lepida S.p.a. Societa' in housedegli enti stessi. Sono inoltre presenti altreRPV secondarie attivate mediante convenzioni Consip o Intercenter con gli operatori aggiudicatari di tali convenzioni

Misure di Sicurezza	Misura Adottata? SI/NO/ PARZIALE	Misura da Adottare? SI/NO	Specifiche
Antivirus	si		Tutte le postazioni informatiche sono dotate di sistema di antivirus mantenuto aggiornato quotidianamente
Crittografia	no	si	E' prevista l'adozione di sistemi di crittografia delle apparecchiature hardware mediante le soluzioni presenti sui sistemi operativi.
Pseudonimizzazione	no	no	
Aggiornamento / Patching Sistema Operativo	si		L'aggiornamento dei sistemi operativi e' schedulato ed automatizzato sulle singole postazioni
Aggiornamento / Patching Applicativo	parziale		L'aggiornamento delle componenti applicative e' garantito per quei sistemi software che consentono l'automatizzazione del processo e per tutti gli applicativi verticali specifici della P.A per i quali l'aggiornamento viene eseguito medianti sistemi manuali/semi automatici/automatici forniti dal produttore
Istruzioni al personale perché non lasci i terminali incustoditi	si		E' stato predisposto un manuale operativo (Regolamento per l'utilizzo dei sistemi informatici al fine di mediante il quale viene istruito il dipendente all'utilizzo dei sistemi informatici al fine di garantire il corretto uso degli stessi, a prevenire la perdita di dati. Vengono inoltre indicatele principali norme comportamentali da tenere.
Blocco dei terminali non utilizzati con ScreenSaver protetto da password personale	si		I sistemi informatici in dotazione agli utenti consento di attivare la protezione mediante ScreenSaver, al fine di garantire la protezione delle dotazioni informatiche ad essi attribuite. I dettagli sono riportati nel Regolamento per l'utilizzo dei sistemi informatici.
Sistemi UPS	si		Tutti i sistemi server sono alimentatiattraverso sistemi UPS
Generatore elettrico	si		Tutti i sistemi server dei due datacenter principali sono alimentati attraverso sistemi UPS. I Server presenti presso i datacenter Locali nei vari comuni sono alimentati da UPS

Misure di Sicurezza	Misura Adottata? SI/NO/ PARZIALE	Misura da Adottare? SI/NO	Specifiche
High Availability	si		I Sistemi presenti presso i due datacenter principali collegati tra loro in Campus sono in HA
Disaster Recovery	Parziale	si	Sono attivi ed in corso di revisione i sistemi che consentono il DR. Verranno formalizzate le procedure al termine dello svolgimento delle attività.

48

4.4 *Valutazione dei rischi generali*

Si riportano di seguito gli elementi di analisi dei rischi tenuto conto dei seguenti fattori:

Rischio: Rischio potenziale valutato

Probabilità: allorchè applicabile

Gravità del rischio: Indica la gravità del danno potenziale causato qualora si verificasse.

Rimedi: Indica se l'azienda ha adottato misure per coprire il rischio o meno.

Fattore di rischio: Indica in definitiva il fattore di criticità e di probabilità legate alla gravità e al danno conseguente

4.5 *Accessi non autorizzati alla struttura*	Fattore	Valore
Descrizione: Non sussiste il controllo gli accessi esterni con un sistema di identificazione all'ingresso. Sussistono le telecamere di videosorveglianza sui tre ingressi principali dei quali normalmente (salvo casi eccezionali) solo uno è adibito ad ingresso del pubblico e dei dipendenti. Le immagini di tali telecamere sono visibili dalla Polizia Locale dell'Unione solo Presidio di Medolla. Sussiste un allarme durante gli orari di chiusura degli uffici.	Probabilità	Bassa
	Gravità	Bassa
	Danno economico	Basso
	Copertura	Media
	Fattore di rischio	Basso
4.6 *Incendio*	**Fattore**	**Valore**
Descrizione: Sussistenza dei mezzi ordinari di spegnimento ai sensi della vigente normativa in materia di sicurezza sui luoghi di lavoro	Probabilità	Media
	Gravità	Media
	Danno economico	Media
	Copertura	Media
	Fattore di rischio	Medio
4.7 *Distruzione o perdita dei dati cartacei*	**Fattore**	**Valore**
Descrizione:	Probabilità	Media

Commentato [CF61]: i

Sussistenza di mezzi per creare delle copie dei dati personali e/o per ripristinare il sistema a seguito di incidente	Gravità	Media
	Danno economico	Medio
	Copertura	Media
	Fattore di rischio	Medio
4.8 Divulgazione dati a soggetti non autorizzati	**Fattore**	**Valore**
Descrizione: Gli archivi cartacei sono contenuti in armadietti chiusi a chiave in uffici non accessibili al pubblico.	Probabilità	Bassa
	Gravità	Bassa
	Danno economico	Basso
	Copertura	Alta
	Fattore di rischio	Basso
4.9 Contagio da virus informatici	**Fattore**	**Valore**
Descrizione: Sussistenza antivirus	Probabilità	Bassa
	Gravità	Bassa
	Danno economico	Basso
	Copertura	Medio
	Fattore di rischio	Medio
4.10 Accessi non autorizzati da rete esterna	**Fattore**	**Valore**
Descrizione: Sussistenza di firewall	Probabilità	Bassa
	Gravità	Bassa
	Danno economico	Basso
	Copertura	Media
	Fattore di rischio	Basso
4.11 Condotte degli operatori	**Fattore**	**Valore**
Descrizione: I dipendenti hanno media conoscenza in materia informatica	Probabilità	Media
	Gravità	Media
	Danno economico	Medio
	Copertura	Media
	Fattore di rischio	Medio

RIFERIMENTI DOCUMENTALI

- **Vulnerability Assessment**
- **Regolamento per l'utilizzo dei sistemi informatici**

5. Contrattualistica Privacy

Il GDPR coinvolgerà tutte le attività di trattamento poste in essere dall'Ente e, inevitabilmente, anche l'ambito dei rapporti con i fornitori dell'Ente, dove sono richiesti adempimenti legati alla regolamentazione, trasparenza e regolarità del flusso dei dati personali trattati per conto dell'Ente, così da considerare e conseguentemente regolamentare gli aspetti legati alla *data protection*.

Nell'ottica del principio di *accountability*, il Titolare ha previsto già a livello di negoziazione e successiva conclusione degli accordi lo schema di gestione dei dati personali, dimostrando in tal modo l'effettiva proattività del titolare rispetto al trattamento.

A tal scopo, il Titolare ha valutato lo status dei contenuti contrattuali esistenti rispetto alle prescrizioni contenute nel GDPR, prevedendo differenti livelli di intervento:

- Clausola generale, da inserire in quelle fattispecie contrattuali a minimo impatto privacy;
- Clausola standard, da utilizzare per categorie assimilabili di contratti e da modulare rispetto all'impatto privacy sull'oggetto contrattuale;
- *Privacy Level Agreement* (PLA), da redigere sulla base di contenuti contrattuali di particolare specificità tecnica;
- *Data Processing Agreement* (DPA), da redigere a fronte di trattamenti di dati personali infragruppo o in caso di contitolarità del trattamento.

RIFERIMENTI DOCUMENTALI

- Analisi contrattualistica

- Clausole contrattuali data protection

6. MOG- Privacy

Il GDPR impone al Titolare del trattamento l'implementazione di misure organizzative idonee a garantire un livello di sicurezza adeguato al rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Il Titolare ha, pertanto, adottato un sistema di gestione privacy a dimostrazione che le persone operanti presso l'Ente effettuando, primariamente o in via residuale, un trattamento di dati personali, sono state sottoposte a procedure organizzative e formative rivolte alla protezione e alla gestione del flusso dei dati.

RIFERIMENTI DOCUMENTALI

- MOG Privacy

7. Integrazione Informative

Attesi i nuovi elementi richiesti dal GDPR a composizione del contenuto delle informative agli interessati, il Titolare del trattamento ha proceduto con le dovute integrazioni, inserendo gli elementi richiesti dalla normativa europea, in particolare:

a) i dati di contatto del DPO, se designato;
b) la base giuridica del trattamento;
c) ove applicabile, gli interessi legittimi perseguiti dal titolare;
d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati;
e) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione intenzionale e l'esistenza delle garanzie appropriate per la sicurezza dei dati;
f) il periodo di conservazione dei dati ovvero i criteri utilizzati per determinare tale periodo;
g) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
h) ove applicabile, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
i) il diritto di proporre reclamo a un'autorità di controllo;
j) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
k) ove applicabile, l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
l) ove applicabile, la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

RIFERIMENTI DOCUMENTALI

- Informative per gli interessati

8. Audit sulle misure tecniche ed organizzative

Al fine di rispettare i canoni di sicurezza così come imposti dal GDPR, il cui articolo 32 individua tra le misure di sicurezza anche "*una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*", il Titolare ha implementato un sistema di audit di quanto adottato nell'ambito del progetto di *compliance* al GDPR.

Ciò al fine di rafforzare la prova *dell'accountability* così come richiesta dalla normativa europea.

9. Revisione

Giova qui rilevare che il presente documento inteso comprensivo dei suoi allegati verrà aggiornato nei seguenti casi, laddove di impatto rispetto ai diritti degli interessati:

- modifiche normative o emanazione di best practices;
- variazioni organizzative e delle attività istituzionali svolte dall'Ente;
- upgrade tecnologici sia sotto il profilo delle funzionalità che dal punto di vista della sicurezza;
- dismissione degli applicativi;
- data breach;
- la necessità di nuove analisi richieste dal DPO.

10. Sottoscrizione

Il presente Registro delle attività di trattamento è stato redatto in ottemperanza alla normativa in materia di protezione del dato personale.

Il sottoscritto _____nella sua qualità di Sindaco e legale rappresentante pro – tempore dell'Ente, procede alla firma del presente documento conferendo la necessaria ufficialità ad esso e alle informazioni contenute.

_____, __/__/____ Per l'Ente

_____

TITOLARE DEL TRATTAMENTO COMUNE DI MEDOLLA	
RESPONSABILI DEL TRATTAMENTO	
AREA AFFARI GENERALI	D.ssa Maria Chiara Grisanti
AREA LAVORI PUBBLICI, PATRIMONIO, AMBIENTE E MANUTENZIONE, PROTEZIONE CIVILE	Geom. Lorenzo Guagliumi
AREA EDILIZIA PRIVATA, URBANISTICA E MUDE	Geom. Alberto Annovi
AREA PROMOZIONE DEL TERRITORIO, CULTURA E TEMPO LIBERO	D.ssa Giorgia Bergonzini
AUTORIZZATI AL TRATTAMENTO (INCARICATI)	
AREA AFFARI GENERALI Servizio Segreteria, Protocollo, Contratti, Archivio Corrente Servizi Demografici e Polizia Mortuaria	Sala Elisa Ferraresi Rita De Luca Rosaria Rebecchi Fabio Barduzzi Katia Aldrovandi Francesco Bonvicini Anna
AREA PROMOZIONE DEL TERRITORIO, CULTURA E TEMPO LIBERO Servizio Commercio e Attività Produttive Servizio Sport, Associazionismo, Volontariato e Anagrafe canina Servizio Cultura, Biblioteca e Archivio Storico Servizio Comunicazione, Europa, Relazioni Internazionali e Intercomunali	Mantovani Enrica Ganzerli Gloria Catellani Viola Ganzerli Guido Tiziano
AREA EDLIZIA PRIVATA, URBANISTICA E MUDE Servizio Urbanistica ed Edilizia Privata	Bergamini Giovanna Veronesi Sara Peri Federica
AREA LAVORI PUBBLICI, PATRIMONIO, AMBIENTE E MANUTENZIONE, PROTEZIONE CIVILE Servizio Lavori Pubblici Servizio Ambiente, Manutenzione (compreso coordinamento operai) e Protezione Civile Servizio Patrimonio	Tartarini Marco Rebecchi Elisa Balisciano Moretti Rosario Balsamo Maria

REGOLAMENTO PER L'UTILIZZO DEI SISTEMI INFORMATICI

Indice generale

Premessa 1
1 - Oggetto e finalità 2
2 - Principi generali e di riservatezza nelle comunicazioni 2
3 - Tutela del lavoratore 3
4 - Campo di applicazione 3
5 - Gestione, assegnazione e revoca delle credenziali di accesso 4
6 - Utilizzo infrastruttura di rete e FileSystem 4
7 - Utilizzo degli Strumenti elettronici 5
8 Utilizzo di internet 6
9 - Utilizzo della posta elettronica 7
10 Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti 8
11 – Assistenza agli utenti e manutenzioni 9
12 - Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16) 10
13 - Conservazione dei dati 11
14 - Partecipazioni a Social Media 12
15 - Comportamenti in caso di Data Breach (Violazione Dati Personali) 12
16 - Norme finali 13

Premessa

Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò PC, notebook, tablet, smartphone, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti Informatici"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti Informatici, nonché le relative reti a cui è possibile accedere tramite gli stessi, sono domicilio informatico dell'Ente.

Nell'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo dell'Azienda il dipendente è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile. Gli strumenti, le reti e le banche dati possono essere utilizzati esclusivamente per ragioni di servizio.

Comportamenti difformi possono causare gravi rischi alla sicurezza ed alla integrità dei sistemi informativi aziendali, sono suscettibili di valutazione ai sensi del codice disciplinare di cui agli articoli 59 e seguenti del CCNL, e possono assumere rilevanza anche sotto il profilo penale.

Le precauzioni di tipo tecnico predisposte dall'azienda possono proteggere le informazioni durante il loro transito fra i sistemi della rete locale, anche quando queste rimangono inutilizzate su un disco di un computer, ma unicamente se presenti su sistemi server; nel momento in cui esse raggiungono fisicamente la postazione dell'utente finale, la loro protezione dipende esclusivamente da quest'ultimo.

L' Azienda garantisce a tutti gli incaricati un adeguato aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati tramite l'utilizzo di elaboratori elettronici e dell'infrastruttura informatica aziendale.

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, le indicazioni per una corretta e adeguata gestione delle informazioni, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente.

Ogni dipendente e collaboratore è tenuto a rispettare il Regolamento, che è reso disponibile tramite le modalità specificate al punto 15.

I dati personali e le altre informazioni dell'Utente registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Per tutela del patrimonio si intende altresì la sicurezza informatica e la tutela del sistema informatico. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

1 - Oggetto e finalità

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";
- in attuazione del Regolamento Europeo 679/16 "General Data Protection Regulation" (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 23 del D.Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti *«dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori»* e di quelli *«utilizzati dal lavoratore per rendere la prestazione lavorativa».*

La finalità è quella di promuovere in tutto il personale una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente sia conforme alle finalità per le quali sono state messe a disposizione del personale e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

2 - Principi generali e di riservatezza nelle comunicazioni

1. I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:
    1. **il principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. 679/16);

2. **i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

2. È riconosciuto al datore di lavoro di potere svolgere attività di monitoraggio, che nella fattispecie saranno svolte solo dall'Amministratore di Sistema o dal personale delegato dall'Amministratore di Sistema, sempre nel rispetto della succitata normativa.
3. Il dipendente si attiene alle seguenti regole di trattamento:
    1. È vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.
    2. È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
    3. È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front office e di ricezione di Clienti / Fornitori o colleghi di lavoro.
    4. Per le riunioni e gli incontri con Clienti, Fornitori, Consulenti e Collaboratori dell'Ente è necessario utilizzare le eventuali / zone sale dedicate.

3 - Tutela del lavoratore

1. Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.
2. È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-77 del Reg. 679/16.

4 - Campo di applicazione

1. Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto.
2. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata come "incaricato del trattamento".

5 - Gestione, assegnazione e revoca delle credenziali di accesso

3. Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Responsabile

dell'ufficio/area nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dalla Direzione o dal Responsabile dell'Ufficio/area con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all'Amministratore di Sistema o al Responsabile di riferimento.

4. Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Amministratore di Sistema, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza senza divulgarla.
5. La password deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole, minuscole, numeri e caratteri speciali. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un familiare).
6. È necessario procedere alla modifica della password a cura dell'utente al primo accesso e, successivamente, almeno ogni tre mesi.
7. Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio/area di riferimento dovrà comunicare formalmente e preventivamente all'Amministratore di Sistema la data effettiva a partire dalla quale le credenziali saranno disabilitate.

6 - Utilizzo infrastruttura di rete e FileSystem

1. Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 5.
2. È assolutamente proibito accedere alla rete ed ai sistemi informativi utilizzando credenziali di altre persone.
3. L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Gli Strumenti Informatici e tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, sms, mail personali, film e quant'altro. Ogni materiale personale rilevato dall'Amministratore di Sistema a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sugli Strumenti viene rimosso secondo le regole previste nel successivo punto 12 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare dell'Amministratore di Sistema e non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C: o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse, poiché non sono garantite la sicurezza e la protezione contro l'eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.
4. Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a device esterni (hard disk, chiavette, CD, DVD e altri supporti).
5. Senza il consenso dell'Amministratore di Sistema è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul Server o sullo Strumento in dotazione) su repository esterne (quali ad esempio Dropbox, Google Drive, OneDrive, WeTransfer,

ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi. In caso di necessità l'Ente dovrà mettere a disposizione modalità in linea con le presenti direttive.

6. Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.
7. L'Ente mette a disposizione dei propri utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno. Tale accesso potrà avvenire mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna o altre modalità congrue allo stesso scopo L'accesso mediante VPN, o altra modalità, viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso mediante VPN, o altra modalità congrua, dovranno seguire le prescrizioni del punto 5.
8. All'interno delle sedi lavorative è resa disponibile anche una rete senza fili, c.d. "WiFi". Tali reti consentono l'accesso alle risorse e ad internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete WiFi viene concesso a consulenti, professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con l'Ente necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e funzionari dell'Ente che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione WiFi sarà effettuata dall'Amministratore di Sistema.
9. L'Amministratore di Sistema si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

7 - Utilizzo degli Strumenti elettronici

1. Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà dell'Ente e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente l'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente /collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.
2. L'accesso agli Strumenti è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dall'Amministratore di Sistema (cfr. 5). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.
3. Gli strumenti informatici devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente all'Amministratore di Sistema ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.
4. Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte dell'Amministratore di Sistema.
5. L'utente è tenuto a scollegarsi dal sistema, o bloccare l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: lasciare un PC 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.

6. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Amministratore di Sistema.
7. È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.
8. È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.
9. È vietato l'utilizzo di supporti di memoria (chiavi USB, CD, DVD o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti, salvo che il supporto utilizzato sia stato fornito o verificato dall'Amministratore di Sistema. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.
10. È vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema (ad esempio, ma non limitatamente a, smartphone, fotocamere, webcam, stampanti).
11. È vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, stampanti, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.
12. Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente è tenuto a comunicarlo tempestivamente all'Amministratore di Sistema.

8 Utilizzo di internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

1. È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner. L'accesso è regolato dal proxy con le sue policy di sicurezza debitamente implementate e aggiornate.
2. È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.
3. È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di Sistema.
4. L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse, potrà contattare l'Amministratore di Sistema per uno sblocco selettivo.
5. Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una mail indirizzata all'Amministratore di Sistema, ed in copia al Dirigente/Capo Servizio, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i punti 13 e 14 del presente regolamento. Al termine dell'attività l'Amministratore di Sistema ripristinerà i filtri alla situazione iniziale.
6. 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 dal al Dirigente/Capo Servizio e dall'Amministratore di Sistema, con il rispetto delle normali procedure di acquisto.

7. È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema e dal Dirigente/Capo Servizio .
8. È assolutamente vietata la partecipazione a Forum non professionali, ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).
9. È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Amministratore di Sistema. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed e-mail. È consentito un utilizzo legato esclusivamente a scopi professionali. Anche su tali strumenti di messaggistica istantanea è attivo il monitoraggio e la registrazione dell'attività degli utenti, secondo le disposizioni dei punti 13 e 14 del presente regolamento.
10. Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc.) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

9 - Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

1. Ad ogni utente viene fornito un account e-mail nominativo, generalmente coerente con il modello *nome.cognome@dominio dell'azienda.* L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.
2. L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati.
3. L'iscrizione a mailing-list o newsletter esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.
4. Allo scopo di garantire sicurezza alla rete, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In qualunque situazione di incertezza contattare l'Amministratore di Sistema per una valutazione dei singoli casi.
5. Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.
6. Nel caso fosse necessario inviare allegati "pesanti" (fino a 10MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati ancora più voluminosi è necessario rivolgersi all'Amministratore di Sistema.

7. Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso criptazione con apposito software (archiviazione e compressione con password). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.
8. Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare, se gli strumenti in dotazione lo consentono, un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente di tipo collettivo, tipo ufficio….@ Dominio_Ente. rivolgersi all'Amministratore di Sistema per tale eventualità.
9. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione auto-reply o l'inoltro automatico su altre caselle e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) per verificare il contenuto di messaggi e per inoltrare al Titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile;
10. La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del Dirigente responsabile competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.
11. È vietato inviare messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione;
12. La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni.
13. I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware e per l'eliminazione dello spam. I messaggi che dovessero contenere virus vengono eliminati dal sistema e il mittente/destinatario puo' essere avvisato mediante messaggio specifico.

10 Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono, sono di proprietà dell'Ente e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

1. Il telefono affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

2. Qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 7 "Utilizzo di personal computer"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8), se consentita.
3. Per gli smartphone è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "app" nel contesto degli smartphone) diverse da quelle autorizzate dall'Amministratore di Sistema.
4. È vietato l'utilizzo dei fax per fini personali, tanto per spedire quanto per ricevere documentazione, fatta salva esplicita autorizzazione da parte del Responsabile di Ufficio.
5. È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio.
6. Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:
    1. Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
    2. Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
    3. Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi
7. Nel caso in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni a persone terze non autorizzate od utilizzare le funzioni di stampa con codice.

11 – Assistenza agli utenti e manutenzioni

1. L'Amministratore di Sistema può accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:
    1. verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale.
    2. verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete.
    3. aggiornamento software e manutenzione preventiva hardware e software.
2. Gli interventi tecnici possono avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, l'Amministratore di Sistema è autorizzato ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.
3. L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.
4. Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o l'Amministratore di Sistema devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

12 - Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

1. Poiché in caso di violazioni contrattuali e giuridiche, sia il datore di lavoro, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi

legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dell'art. 2.2 del presente Regolamento e dei seguenti principi:

1. **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi.
2. **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti.
3. **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

2. L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti al punto 12.3 e 12.4) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli Strumenti.

3. **Controlli per la tutela del patrimonio comunale, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).**

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali per il tramite dell'Amministratore di Sistema, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).

1. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento.
2. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 6 – 7 – 8 – 9 con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo del numero IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite.

Qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Responsabile del Trattamento, unitamente all'Amministratore di Sistema, potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia prendendo tutte le misure tecnicamente necessarie alla soluzione del problema.

4. ***Controlli per esigenze produttive e di organizzazione***
    1. Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.
    2. Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali, per il tramite dell'Amministratore di Sistema, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo).
    3. Redazione di un atto da parte del Dirigente e/o Responsabile Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento.
    4. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore oppure tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali.
    5. Redazione di un verbale che riassuma i passaggi precedenti.
    6. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro.
    7. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection Regulation".

13 - Conservazione dei dati

1. In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro al massimo 365 giorni dalla loro produzione.
2. In casi eccezionali – ad esempio: per esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria – è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra esplicitate.
3. L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

14 - Partecipazioni a Social Media

1. L'utilizzo a fini promozionali e commerciali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali, (ed altri siti o social media) è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.
2. Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio, anche immateriale, quanto i propri collaboratori, i propri clienti e

fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

3. Il presente articolo deve essere osservato dall'Utente sia che utilizzi dispositivi messi a disposizione dall'Ente, sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.
4. La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Ente. L'utente, nelle proprie comunicazioni, non potrà quindi inserire il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione.
5. L'utente deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori, se non con il preventivo personale consenso di questi, e comunque non potrà postare nei social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile d'ufficio.
6. Qualora l'utente intenda usare social network, blog, forum su questioni anche indirettamente professionali (es. post su prodotti, servizi, fornitori, partner, ecc.) egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

15 - Comportamenti in caso di Data Breach (Violazione Dati Personali)

COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?*

Una 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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il dipendente deve, in caso di sospetta violazione di dati personali segnalare immediatamente al responsabile del trattamento il potenziale rischio. Sara' poi compito di quest'ultimo verificare

ed eventualmente notificare al garante in conformita al Regolamento (UE) 2016/679 l'avvenuto Breach.

16 - Norme finali

1. La pubblicazione, a cura dell'Amministratore di Sistema, avverrà nelle seguenti forme: trasmissione per posta elettronica interna a tutti i Dirigenti Responsabili, e a tutti gli impiegati provvisti di e-mail; Comunicazione in fase di assunzione da parte dell'Ufficio Personale; Pubblicazione sulla rete intranet quindi attraverso la rete informatica interna, mediante affissione nei luoghi di lavoro con modalità analoghe a quelle previste dall'art. 7 dello Statuto dei lavoratori.
2. T
   u
   t
   t
   i

   g
   l
   i

   u
   t
   e
   n
   t
   i

   p
   o
   s
   s
   o
   n
   o

   p
   r
   o
   p
   o
   r
   r
   e

   i
   n
   t
   e
   g
   r
   a
   z
   i
   o
   n
   i

VA UCMAN

Unione Comuni Modenesi Area Nord

Presentazione dei risultati

VA ambienti esterni

UCMAN

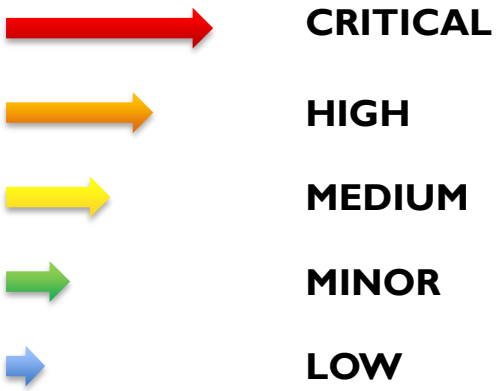
OBIETTIVO:
Proteggere UCMAN

Forniamo al management il punto di vista di un attaccante evidenziando i punti deboli da mettere in sicurezza

Risultati Vulnerability Assessment

Vulnerability Assessment

Valorizzazione dei
requisiti relativi
all'impatto sul business



Il VA è stato effettuato sul perimetro esterno dell'organizzazione

Numerosità per impatto delle vulnerabilità sul perimetro esterno

Active Hosts: 9

Hosts Matching Filters: 8

Total: 133 Security Risk (Avg): 3.2 Business Risk (Avg): 25/100

Security Risk (Avg): is the average security risk for all active hosts.

Business Risk (Avg): is the average business risk for all active hosts.

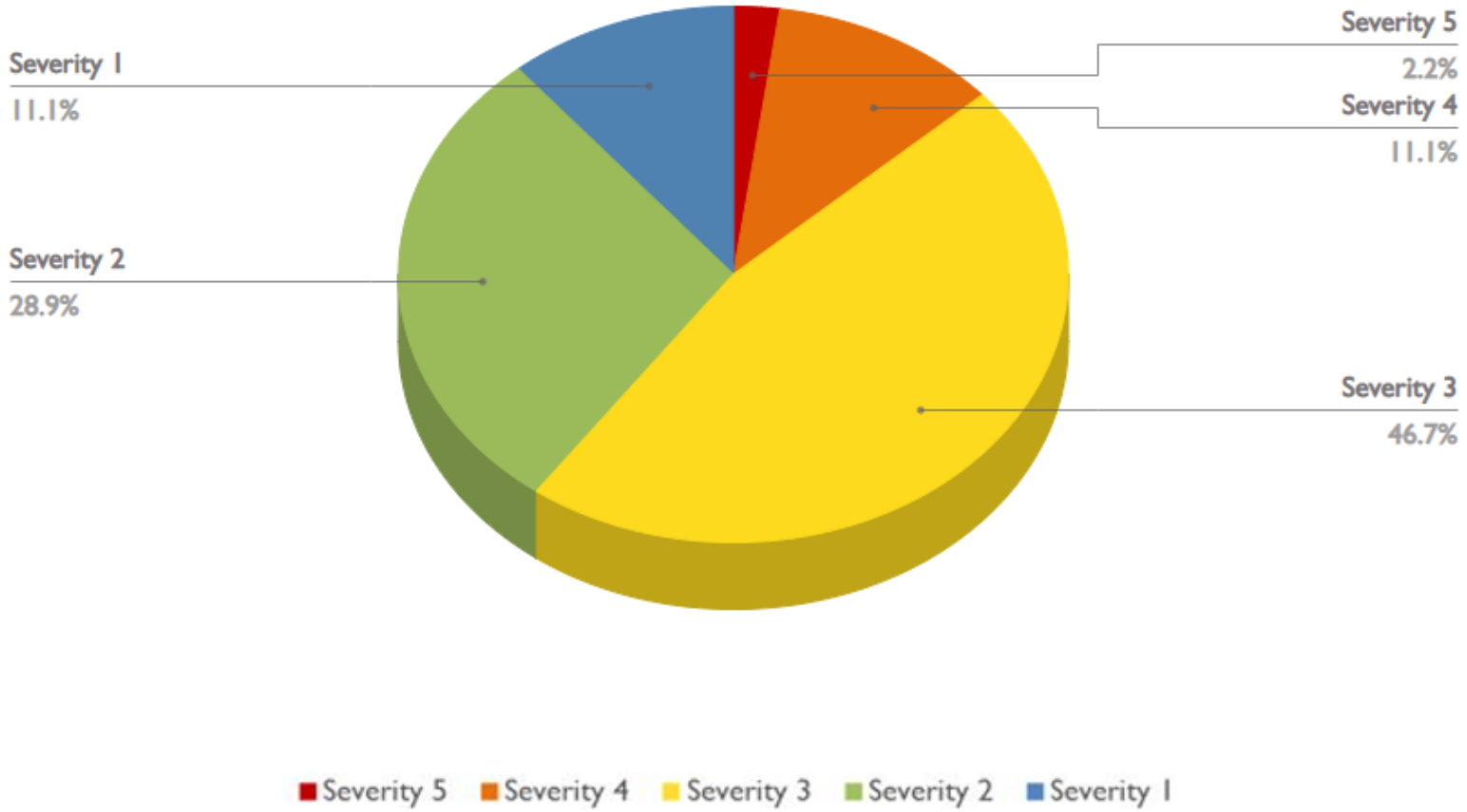
Security Risk: is the highest severity level detected for each hosts.

Business impact: identifies which hosts are most critical to organization.

Business Risk: is calculated as the product of Security Risk by Business Impact for each hosts.

Open report

Vulnerabilità sul perimetro esterno



Vulnerabilità critiche presenti sul perimetro esterno

Comunicazione non autenticata via SSL

mx.comune.finale-emilia.mo.it (195.62.173.83)

Nel caso un aggressore riuscisse a sfruttare questa vulnerabilità potrebbe impersonare il server. Si evidenzia una vulnerabilità su protocollo SSL versione 3 che di default permette una comunicazione non autenticata tra client e server.

SOLUZIONE: Si consiglia di disabilitare l'autenticazione anonima.

Attacco TLS ROBOT consentito

mx.comune.finale-emilia.mo.it (195.62.173.83)

Lo sfruttamento di questa vulnerabilità consente a un utente malintenzionato di ottenere la chiave RSA necessaria per decifrare il traffico TLS in determinate condizioni.

SOLUZIONE: Si consiglia di applicare la patch per correggere la vulnerabilità.

Chiavi deboli ammesse per protocollo SSL/TLS

smtp-01.unioneareanord.mo.it (195.62.174.132)
mx.comune.finale-emilia.mo.it (195.62.173.83)
195.62.174.139

Lo scambio di chiavi per le sessioni SSL/TLS può essere eseguito utilizzando chiavi deboli, un malintenzionato potrebbe intercettare i pacchetti e violare le primitive crittografiche decifrando il contenuto della sessione

SOLUZIONE: Si consiglia di modificare la configurazione dei server ed imporre l'utilizzo di chiavi di almeno 2048 bit per gli algoritmi RSA e Diffie Hellman.

Utilizzo di un canale di comunicazione non sicuro

mx.comune.finale-emilia.mo.it (195.62.173.83)

Un utente malintenzionato può sfruttare questa vulnerabilità per leggere comunicazioni protette o modificare in modo dannoso i messaggi.

SOLUZIONE: Si consiglia di disabilitare il protocollo SSLv2 e di utilizzare un canale di comunicazione cifrato con protocollo di cifratura di tipo TLS (almeno dalla versione 1.2).

PHP consente l'esecuzione di codice arbitrario

195.62.174.136
195.62.174.139

Sfruttando la console di gestione dei modelli tramite un accesso abusivo la versione PHP 5.6.1 consente l'esecuzione di codice arbitrario

SOLUZIONE: Si consiglia aggiornare PHP all'ultima versione disponibile.

Autenticazione in chiaro consentita

195.62.174.136

Una form per l'accesso è disponibile su protocollo HTTP, intercettando i pacchetti durante il processo di autenticazione è possibile ottenere le credenziali in chiaro

SOLUZIONE: Si consiglia di utilizzare esclusivamente il protocollo HTTPS per le pagine di autenticazione

Versioni vulnerabili di software di terze parti

Alcuni degli applicativi interessati sono:

- ISC BIND
- OpenSSL
- PHP

Open report sorted by vulnerability

Nel caso un aggressore riuscisse a sfruttare le vulnerabilità delle attuali versioni dei software potrebbe riuscire a prendere il controllo dei sistemi su cui sono installati e ad eseguire codice arbitrario, compromettendo le proprietà fondamentali di sicurezza informatica (CIA).

SOLUZIONE: Si consiglia di scaricare ed installare le patch per correggere le vulnerabilità per le singole applicazioni.

UCMAN espone alcune vulnerabilità critiche nella rete esterna che permettono la compromissione dei sistemi informativi.

Open report sorted by vulnerability

Cyber Security Remediations

1. Attuare piano di remediation per il riposizionamento delle criticità identificate, in particolar modo quelle di severity Critical ed High;
2. Tenere costantemente aggiornati tutti i componenti software per ridurre il rischio di esposizione a nuove potenziali vulnerabilità;
3. Prevedere un'attività di Penetration Test almeno con cadenza annuale;
4. Pianificare un'attività di Vulnerability Assessment periodica;
5. Prevedere un piano di aggiornamento al fine di dismettere i sistemi operativi obsoleti come Windows Server 2008, a favore delle nuove versioni più recenti, come Windows Server 2019.

www. ificonsulting.eu