ORGANIGRAMMA "PRIVACY"
ai sensi del Regolamento UE 679/2016 (GDPR)

1 TITOLARE DEL TRATTAMENTO DATI

1.1 Titolare del trattamento dati è 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.

1.2 Titolare del trattamento è quindi l'Unione di Comuni VERONA EST*,* e le funzioni di titolare sono esercitate dal Presidente pro tempore in qualità di legale rappresentante.

1.3 Il Titolare del trattamento, attraverso il suo legale rappresentante (Presidente) provvede a:

a) definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento dei dati personali, provvedendo alla definizione degli obiettivi strategici ed operativi nel DUP e negli altri documenti di programmazione e pianificazione;
b) mettere in atto misure tecniche e organizzative adeguate per garantire che i trattamenti siano effettuati in modo conforme al Codice Privacy ed al GDPR;
c) delegare e/o attribuire, con proprio atto, in tutto o in parte le funzioni ed i poteri del titolare di trattamento, a personale dell'ente adeguatamente formato ed istruito;
d) formare e aggiornare l'elenco dei soggetti designati al trattamento dei dati ed eventualmente pubblicarlo sul sito web istituzionale dell'ente;
e) istituire il ruolo organizzativo di "Responsabile privacy" all'interno dell'ente ed attribuirlo a personale adeguatamente formato ed istruito;
f) designare, con proprio atto, il Responsabile per la protezione dei dati personali (DPO) o fornire linee di indirizzo per l'affidamento del servizio all'esterno;
g) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
h) favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
i) favorire l'adesione a meccanismi di certificazione;
j) assolvere agli obblighi nei confronti del Garante nei casi previsti dalla vigente normativa.

2 CONTITOLARE DEL TRATTAMENTO DEI DATI

2.1 Il *titolare* del trattamento si trova in rapporto di contitolarità con altri titolari quando le finalità e i mezzi del trattamento sono definiti di comune accordo fra le parti.
2.2 I contitolari sono tenuti a determinare, in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.
2.3 L'accordo può designare un punto di contatto per gli interessati.
2.4 L'accordo interno deve riflettere adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati.
2.5 Il contenuto essenziale dell'accordo è messo a disposizione degli interessati. Indipendentemente dalle disposizioni dell'accordo interno, gli interessati possono esercitare i propri diritti nei confronti di e contro ciascun Titolare del trattamento.

3 RESPONSABILE DELLA TRANSIZIONE DIGITALE

3.1 Il Sindaco designa, tra le posizioni apicali dell'ente, un responsabile della transizione digitale, a cui sono attribuiti, i seguenti compiti:

a) pianificare e coordinare lo sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
b) indirizzare e coordinare lo sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
c) indirizzare, pianificare, coordinare e monitorare la sicurezza informatica relativamente ai dati, ai sistemi ed alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1 del d.lgs 82/2005 (dpcm 13.11.2014) ;
d) garantire l'accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
e) analizzare periodicamente la coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
f) cooperare alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
g) indirizzare, coordinare e monitorare la pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h) progettare e coordinare le iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a soggetti giuridici mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
i) promuovere le iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
j) pianificare e coordinare il processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis del d.lgs 82/2005;
k) *j-bis)* pianificare, coordinare ed eventualmente gestire gli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b) d.lgs. 82/2005 (CAD), ed eventualmente gestire i budget assegnati;

Oltre ai compiti sopra indicati, previsti dall'articolo 17 del CAD, al Responsabile della Transizione Digitale sono attribuiti i seguenti compiti:

l) proporre ed eventualmente gestire i budget assegnati per mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati personali sia effettuato conformemente al GDPR, alla normativa nazionale, alle regole deontologiche allegate al Codice Privacy ed alle linee guida del Garante;
m) nominare gli amministratori di sistema definendone compiti, funzioni e responsabilità o attribuendo gli incarichi all'esterno con apposito contratto di servizio;
n) tenere l'elenco degli amministratori di sistema anche esterni;
o) controllare e supervisionare l'attività degli altri amministratori di sistema, soprattutto esterni, valutandola anche attraverso l'esame della relazione annuale predisposta dagli stessi;
p) costituire tavoli di coordinamento con le altre posizioni apicali ed emettere circolari negli ambiti di propria competenza (digitalizzazione ed eventualmente privacy e protezione dei dati).

3.2 Il Responsabile della Transizione Digitale è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde, con riferimento ai compiti relativi alla transizione alla modalità digitale, direttamente all'organo di vertice politico.

3.3. Il Responsabile della transizione digitale è posto a capo di un'unità organizzativa dedicata oppure di un'unità organizzativa esistente, e può essere affiancato da supporti esterni. L'ufficio per la transizione digitale può essere gestito anche in forma associata fra più enti.

4 RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD) - DATA PROTECTION OFFICER (DPO)

4.1 Il Presidente, in qualità di legale rappresentante del Titolare designa il Responsabile della protezione dei dati (d'ora in poi anche RPD o DPO) in caso di attribuzione del ruolo a soggetti interni all'ente, oppure, anche attraverso una delibera di Giunta Unione, fornisce indirizzi al Responsabile della Transizione Digitale o al Referente Privacy per l'affidamento del servizio all'esterno.

4.2 Il RPD/DPO svolge i seguenti compiti:

a) informa e fornisce consulenze al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti in tema di protezione dei dati;
b) verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
c) fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorveglia i relativi adempimenti;
d) funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
e) funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva.

4.3 Al DPO possono essere affidati anche altri compiti / funzioni che non siano incompatibili con il ruolo e che non determinino conflitto di interessi.

4.4 Il RPD/DPO deve essere in possesso di:

a) una conoscenza specialistica della normativa e delle prassi di gestione dei dati personali;
b) un'adeguata conoscenza delle procedure e delle norme che regolano il funzionamento degli enti locali;
c) deve adempiere alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse.

4.5 Il RPD/DPO è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

4.6 Il Titolare del trattamento mette a disposizione del DPO le risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti.

4.7 Il DPO riporta direttamente al Titolare del trattamento e quindi al Sindaco e si interfaccia con il Responsabile della Transizione Digitale ed il Referente privacy

5 REFERENTE PRIVACY

5.1 Il Presidente, in qualità di legale rappresentante del Titolare dei trattamenti, nomina il Referente privacy attribuendogli la titolarità della posizione organizzativa.

5.2 Il ruolo di Referente privacy di norma, coincide con il ruolo/posizione organizzativa di Responsabile della transizione digitale o può essere assegnato ad un soggetto che ricopra una posizione apicale. I due ruoli/posizioni organizzative possono essere posti al vertice di un'autonoma unità organizzativa oppure essere integrati all'interno di un'unità organizzativa esistente. Potranno eventualmente essere anche oggetto di gestione associata.

5.3 Spettano al Referente privacy, a titolo esemplificativo, i seguenti compiti, funzioni, poteri attribuiti/delegati

dal sindaco con l'atto di nomina:

a) proporre gli obiettivi strategici ed operativi per il costante adeguamento dell'organizzazione ai dettati del GDPR, alla normativa nazionale, alle regole deontologiche allegate al Codice Privacy ed alle linee guida del Garante, proponendo l'inserimento di tali obiettivi strategici e/o operativi nel DUP e negli altri documenti di programmazione e pianificazione del Titolare;
b) coordinare l'attività dei titolari di P.O. nello svolgimento delle funzioni e dei compiti in ordine ai processi, procedimenti, e adempimenti relativi al trattamento dei dati personali, alla sicurezza e alla formazione, fornendo ad essi le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
c) formare e aggiornare l'elenco dei designati, dal Titolare a trattare i dati personali e dei soggetti autorizzati ed eventualmente a pubblicarlo sul sito web istituzionale del Titolare;
d) gestire il procedimento di affidamento all'esterno del ruolo di DPO sulla base degli indirizzi stabiliti dal Sindaco o dalla Giunta Comunale;
e) effettuare, anche in collaborazione con il RTD e DPO, periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione dei dipendenti;
f) favorire l'adesione a codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi;
g) favorire l'adesione a meccanismi di certificazione;
h) gestire, unitamente al DPO, i contatti con gli interessati che intendono esercitare i diritti garantiti dal GDPR;
i) gestire, unitamente al DPO, i contatti con il Garante privacy.

6 PREPOSTI AL TRATTAMENTO DEI DATI

6.1 Il Titolare del trattamento, conferisce al personale titolare dei ruoli organizzativi apicali o di unità organizzativa di massima dimensione il ruolo di "*preposto al trattamento dei dati*" (dell'unità organizzativa di cui è responsabile), d'ora in poi solo *preposto*, attribuendo almeno i sotto indicati compiti, funzioni, ed i correlati poteri.

6.2 La nomina dei "*preposti*" avviene con apposito provvedimento del Presidente pro tempore. Tale nomina può essere inserita anche nell'atto di attribuzione del ruolo organizzativo di vertice (ruolo dirigenziale / posizione organizzativa).

6.3 Il provvedimento di nomina a *preposto* deve contenere l'indicazione dei compiti e delle responsabilità che sono affidate con la nomina

6.4 Il provvedimento di nomina a *preposto* comporterà l'attribuzione almeno dei seguenti compiti, funzioni, poteri e responsabilità:

a) trattare i dati personali su istruzione del Titolare del trattamento;
b) garantire che le persone addette o autorizzate al trattamento dei dati personali appartenenti all'unità organizzativa da questi diretta si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) garantire il tempestivo ed integrale rispetto dei doveri del Titolare previsti dal Codice, compreso il profilo relativo alla sicurezza del trattamento così come disciplinato nell'art. 32 del GDPR;
d) osservare le disposizioni contenute negli atti generali di organizzazione dell'ente nonché le specifiche istruzioni impartite dal Titolare;
e) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto

professionale, fermo restando quanto previsto dalla normativa vigente, dalle disposizioni del Garante, dalle disposizioni contenute negli atti generali di organizzazione adottati dall'ente, con particolare riguardo a tutte le disposizioni di rango speciale che comunque incidono sul trattamento dei dati;

f) collaborare con il Titolare del trattamento nella predisposizione del documento di valutazione d'impatto sulla protezione dei dati e nella definizione del Registro delle attività di trattamento, in collaborazione con l'Amministratore/i di sistema e con le altre strutture competenti del Titolare;
g) curare l'elaborazione e la raccolta della modulistica e delle informative, da utilizzarsi all'interno della struttura organizzativa diretta per l'applicazione del Codice, del GDPR, e degli altri atti di natura generale;
h) assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato per quanto previsto nella normativa vigente;
i) assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva) tenendo conto della natura del trattamento e delle informazioni a disposizione;
j) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Codice, dal GDPR e dal presente atto;
k) contribuire alle attività di verifica del rispetto del Codice, del GDPR e del presente atto, comprese le ispezioni realizzate dal Titolare o da un altro soggetto da questi incaricato;
l) curare la costituzione e l'aggiornamento degli archivi/banche dati di competenza, a solo titolo esemplificativo: (i) elenco dei contitolari, elenco dei responsabili dei trattamenti, elenco dei designati autorizzati con i relativi punti di contatto; (ii) elenco hardware e software in uso all'ente;
m) garantire l'aggiornamento della ricognizione dei trattamenti;
n) fornire tutte le necessarie informazioni e prestare assistenza al Responsabile della protezione dei dati (RPD/PDO) nell'esercizio delle sue funzioni.

6.5 Ciascun Dirigente / Titolare di posizione organizzativa nell'espletamento dei compiti, funzioni e poteri delegati o per i quali ha ricevuto la nomina, è obbligato a

a) comunicare tempestivamente, l'inizio di ogni nuovo trattamento, la cessazione o la modifica dei trattamenti in atto, nonché ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio;
b) comunicare la cessazione dei contratti di appalto che comportano trattamento dei dati ed assicurarsi che l'ex responsabile abbia cancellato i dati;
c) collaborare con il Titolare nella redazione della valutazione d'impatto sulla protezione dei dati e nella consultazione preventiva;
d) predisporre le informative previste e verificarne il rispetto;
e) fornire le informazioni necessarie per l'aggiornamento del registro dei trattamenti;
f) designare gli addetti e gli autorizzati al trattamento, e fornire loro specifiche istruzioni;
g) rispondere alle istanze degli interessati secondo quanto stabilito dal Codice e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
h) garantire che tutte le misure di sicurezza riguardanti i dati del Titolare siano applicate all'interno della struttura organizzativa del Titolare ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali responsabili del trattamento;
i) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

6.6 Ciascun Titolare di posizione organizzativa risponde al Titolare del trattamento di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente e della mancata attuazione delle misure di

sicurezza.

6.7 I preposti sono destinatari di interventi di formazione e di aggiornamento obbligatoria per almeno n. 2 (due) ore all'anno.

7 ADDETTI AL TRATTAMENTO DEI DATI PERSONALI DIPENDENTI DEL TITOLARE

7.1 Gli "*addetti al trattamento dei dati*", d'ora in poi solo addetti, sono le persone fisiche, di norma, dipendenti del Titolare del trattamento, designati dai "preposti" a svolgere le operazioni di trattamento dei dati personali di competenza dell'unità organizzativa in cui sono incardinati.

7.2 La designazione di *addetto* al trattamento dei dati personali è di competenza del *preposto* al trattamento dei dati dell'unità organizzativa di competenza che di norma è il dirigente o la posizione organizzativa responsabile dell'unità organizzativa.

7.3 La designazione è effettuata per iscritto (di norma con determina) e individua specificatamente i compiti spettanti all'*addetto* e le modalità cui deve attenersi per l'espletamento degli stessi e l'ambito del trattamento consentito.

7.4 A prescindere dalla formale attribuzione dell'incarico di addetto o soggetto autorizzato, si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale risulti individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Per effetto di tale disposizione, ogni dipendente preposto ad un determinato ufficio/servizio, tenuto ad effettuare operazioni di trattamento nell'ambito di tale servizio, è da considerare, "autorizzato" ai sensi dell'art. 2 quaterdecies del Codice.

7.5 Gli *addetti* ricevono dai *preposti* idonee ed analitiche istruzioni, anche per gruppi omogenei di funzioni, riguardo le attività sui dati affidate e gli adempimenti a cui sono tenuti.

7.6 Gli *addetti* collaborano con i *preposti* e con gli altri organi individuati dal Titolare segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo. In particolare, gli incaricati devono assicurare che, nel corso del trattamento, i dati siano:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, e successivamente trattati in modo compatibile con tali finalità;
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità pel quali i dati sono trattati;
f) trattati in modo tale che venga ad essere garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure organizzative e tecniche adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale.

7.7 Gli *addetti* sono tenuti alla completa riservatezza sui dati di cui siano venuti a conoscenza in occasione dell'espletamento della propria attività, impegnandosi a comunicare i dati esclusivamente ai soggetti indicati dal Titolare e/o dal *preposto* in base alle istruzioni ricevute o in base agli generali di organizzazione

7.8 Gli *addetti* dipendenti del Titolare sono destinatari degli interventi di formazione e di aggiornamento obbligatorio per almeno n. 2 (due) ore annue.

8 AUTORIZZATI AL TRATTAMENTO NON DIPENDENTI DEL TITOLARE

8.1 Gli "*autorizzati al trattamento* dei dati", d'ora in poi solo autorizzati, sono generalmente soggetti a cui, di norma, è concesso effettuare solo alcune tipologie di trattamenti generalmente consultazione o uso dei dati ma non inserimento o modifica delle banche dati e dei relativi dati personali.

8.2 La designazione di "*autorizzato*" al trattamento avviene con atto del legale rappresentante dell'ente o con atto del preposto competente e deve contenere le istruzioni e le modalità di espletamento delle operazioni di trattamento

8.3 Gli *autorizzati* devono essere destinatari di interventi di formazione a meno che il soggetto che autorizza il trattamento (legale rappresentante o preposto) attesti l'adeguata competenza in tema di trattamento dei dati del soggetto autorizzato.

9 AMMINISTRATORE DI SISTEMA

9.1 Per "Amministratore di sistema" si devono intendere quelle figure professionali (interne o esterne all'ente) che hanno il compito di provvedere alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti.

9.2 Gli Amministratori di sistema, a titolo esemplificativo, possono essere così classificati

- ***amministratori di dominio****:* si tratta degli Amministratori dei domini Active Directory interni ed esterni; rientrano in questa categoria i componenti dei gruppi "Domain Admins" e tutti coloro che, attraverso un meccanismo di delega, hanno la possibilità di agire su un sottoinsieme degli oggetti dei domini;
- ***amministratori di server***: si tratta degli utenti che hanno diritti amministrativi su uno o più server; rientrano in questa categoria, a titolo esemplificativo, gli utenti appartenenti al gruppo "Administrators" di uno o più server Windows o gli utenti di uno o più server Linux che, attraverso il comando "sudo", possono impersonare l'utente "root";
- ***amministratori di basi di dati****:* rientrano in questa categoria gli utenti che hanno la possibilità di manipolare la struttura di uno o più database attraverso comandi di "Data Definition Language";
- ***amministratori di apparati di rete***: rientrano in questa categoria gli utenti che hanno la possibilità di accedere ad apparati di rete layer 2 o layer 3 e modificarne le configurazioni;
- ***amministratori di apparati di sicurezza***: rientrano in questa categoria gli utenti che possono modificare le configurazioni di sistemi hardware o software dedicati alla sicurezza, quali ad esempio firewall, sistemi di intrusion prevention, web proxy e sistemi antivirus
- ***amministratori di software complessi****:* rientrano in questa categoria gli utenti che possono agire sui software in uso (ad esempio il gestionale, il software per la fatturazione ecc.) ma che non hanno acceso a credenziali amministrative del server su cui operano
- ***amministratori dei sistemi di backup****:* rientrano in questa categoria gli utenti che gestiscono ed implementano le operazioni di backup e che sovrintendono al loro corretto funzionamento.

9.3 Sulla scorta delle indicazioni ed in collaborazione con il Responsabile della transizione Digitale agli Amministratori di sistema, in base alle diverse competenze assegnate, spettano, di norma, i seguenti compiti:

a) Gestire il sistema informativo-informatico inteso come complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni personali, attenendosi anche alle disposizioni del Titolare in tema di sicurezza.
b) Predisporre ed aggiornare un sistema di sicurezza informatico tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle

persone fisiche, mettendo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, misure che comprendono, tra le altre, se del caso:

(i) la pseudonimizzazione e la cifratura dei dati personali;

(ii) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

(iii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

(iv) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

c) Collaborare nella predisposizione del Piano protezione dati per la parte concernente il sistema informatico ed il trattamento informatico dei dati.
d) Elaborare e tenere aggiornato un disciplinare tecnico da portare in approvazione al Titolare del trattamento in cui siano disciplinati le misure e le procedure di sicurezza aziendali in tema di gestione del sistema informativo-informatico.
e) Elaborare e tenere aggiornato un disciplinare tecnico per la gestione della posta elettronica ed internet.
f) Elaborare e tenere aggiornato un sistema di valutazione dei rischi.
g) Cooperare nella predisposizione della Valutazione d'impatto sulla protezione dati ai sensi dell'articolo 35 del Regolamento (anche DPIA – data protection impact assessement).
h) Collaborare con il titolare e gli altri ruoli dell'organigramma privacy in caso di data breach.
i) Redigere una relazione annuale sull'attività svolta in modo da permetterne la verifica.
j) Vigilare sugli interventi informatici effettuati sul sistema informativo-informatico dell'ente e sull'impianto di videosorveglianza effettuati da vari operatori esterni ed in caso di anomalie segnalarle al Referente / Coordinatore privacy ed al Responsabile Protezione Dati / DPO (Data protection officier).
k) Coordinare assieme al Titolare, al Responsabile Protezione Dati ed al Referente / Coordinatore privacy le attività operative degli addetti ai trattamenti informatici nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento dei dati personali nell'ambito del sistema informatico.
l) Collaborare con il Titolare ed il DPO per l'attuazione delle prescrizioni impartite dal Garante.
m) Comunicare prontamente al Titolare qualsiasi situazione di cui sia venuto a conoscenza che possa compromettere il corretto trattamento informatico dei dati personali.
n) Verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi di elaboratore installati nei pc. presenti nell'unità produttiva.
o) Adottare e gestire sistemi idonei alla registrazione degli accessi logici (autenticazione informatica), sistemi di elaborazione e sistemi di archiviazione elettronica da parte di tutte le persone qualificate amministratori di sistema. Le registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (*log in e log out*) che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;
p) assegnare e gestire il sistema di autenticazione informatica secondo le modalità indicate nel Disciplinare tecnico, e quindi, fra le altre, generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate, le parole chiave ed i Codici identificativi personali da assegnare agli incaricati del trattamento dati, svolgendo anche la funzione di custode delle copie delle credenziali;
q) procedere, più in particolare, alla disattivazione dei Codici identificativi personali, in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 (sei) mesi;
r) adottare adeguati programmi antivirus, firewall ed altri strumenti software o hardware atti a garantire la massima misura di sicurezza tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come

anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche in conformità allo stesso Disciplinare tecnico;

s) adottare tutti i provvedimenti e le azioni necessari ad evitare la perdita o la distruzione, anche solo accidentale, dei dati personali e provvedere al ricovero periodico (*disaster recovery*) degli stessi con copie di *back-up*, vigilando sulle procedure attivate in struttura. L'Amministratore di sistema dovrà anche assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;

t) indicare al personale competente o provvedere direttamente alla distruzione e smaltimento dei supporti informatici di memorizzazione logica o alla cancellazione dei dati per il loro reimpiego, alla luce del Provvedimento del Garante per la Protezione dei Dati personali del 13 ottobre 2008 in materia di smaltimento strumenti elettronici;

9.4 I (diversi) ruoli di amministratore di sistema possono essere assegnati ad uno o più dipendenti dell'ente oppure, in caso di mancanza di professionalità adeguate all'interno, affidati all'esterno attraverso uno o più contratti di prestazione di servizi.