COMUNE DI BELLUSCO

Provincia di Monza e della Brianza (MB)

ORIGINALE

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

N° 56 del 24/07/2018

OGGETTO:	**STATO DI ATTUAZIONE NEL COMUNE DI BELLUSCO DEL NUOVO REGOLAMENTO EUROPEO N.679/2016 SULLA PROTEZIONE DEI DATI PERSONALI.**

Il giorno **ventiquattro,** del mese di **Luglio**, dell'anno 2018 alle ore **21:00,** presso questa sede comunale, convocati previa osservanza di tutte le formalità prescritte dal vigente Statuto comunale, gli Assessori comunali si sono riuniti per deliberare sulle proposte di deliberazione iscritte all'ordine del giorno ad essi consegnato.
Assume la presidenza **il Vice Sindaco Arch. Mauro Colombo**.
Assiste la seduta **il Segretario Comunale Pepe Dott.ssa Lucia.**

Dei Signori componenti la Giunta Municipale di questo Comune:

Cognome e Nome	Qualifica	Presente
INVERNIZZI ROBERTO	Sindaco	
COLOMBO MAURO	Assessore	X
BENVENUTI MARIA	Assessore	X
MISANI DANIELE	Assessore	X
STUCCHI FRANCESCO MARIO	Assessore	

Totale Presenti: 3 Totale Assenti: 2

Il Presidente, accertato il numero legale per poter deliberare validamente, invita la Giunta Comunale ad assumere le proprie determinazioni sulla proposta di deliberazione indicata in oggetto:

OGGETTO:	STATO DI ATTUAZIONE NEL COMUNE DI BELLUSCO DEL NUOVO REGOLAMENTO EUROPEO N.679/2016 SULLA PROTEZIONE DEI DATI PERSONALI.

LA GIUNTA COMUNALE

PREMESSO che il Parlamento Europeo ed il Consiglio, in data 27 aprile 2016, hanno approvato il Regolamento Generale sulla protezione dei dati personali (RGPD) n. 679 e che lo stesso, pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016, è diventato definitivamente applicabile in tutti i Paese UE a partire dal 25 maggio 2018;

DATO ATTO che l'Italia ha recepito i nuovi principi attraverso l'art. 13 della legge 163/2017, entrata in vigore il 21 novembre 2017, che ha attribuito al Governo la delega ad adottare (entro 6 mesi) uno o più provvedimenti rivolti a:

- abrogare le disposizioni del D.lgs. 196/2003 (l'attuale Codice Privacy) che siano in contrasto o comunque incompatibili con la nuova disciplina europea in tema di trattamento di dati personali e a modificarlo al fine di dare puntuale attuazione alle disposizioni del RGPD;
- valutare l'opportunità di avvalersi dei poteri specifici del Garante per la protezione di dati personali (Garante Privacy) affinché adotti provvedimenti attuativi e integrativi volti al perseguimento delle finalità previste dal RGPD;
- adeguare l'attuale regime sanzionatorio, a livello penale ed amministrativo, alle disposizioni del RGPD, al fine di garantire la corretta osservanza della nuova normativa;

CONSIDERATO che tali decreti legislativi non sono stati ancora approvati, ma che il Regolamento europeo è direttamente applicabile negli Stati membri ed è entrato in vigore il 25 maggio 2018;

DATO ATTO che il Comune di Bellusco si è attivato per dare attuazione al Regolamento Europeo 679/2016 ed con determinazione del responsabile del Settore Amministrativo n. 89/2018 è stato affidato il servizio relativo agli interventi di adeguamento del sistema di gestione della privacy del Comune alle disposizioni del nuovo regolamento europeo sul trattamento dei dati ed incarico per il Responsabile della Protezione dei dati (RPD)/Data Protection Officer (DPO) per i Comuni di Bellusco e Mezzago e per l'Unione;

DATO ATTO che il regolamento UE 679/2016 individua tre figure chiave:

- Il titolare del trattamento che negli Enti Locali è il Sindaco quale rappresentante legale dell'Ente, definito dall'art. 4, punto 7, del regolamento UE 679/2016 come la "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";
- Il responsabile del trattamento, definito dall'art.4, punto 8, del regolamento UE 679/2016 "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento". All'art. 28 del regolamento si prescrive che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo [ricorra] unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato". Pertanto può essere nominato responsabile un dipendente dell'Ente, oppure può essere incaricato, anche mediante contratto d'appalto di servizi un soggetto esterno, persona fisica o giuridica. Il titolare del trattamento, ovvero il Sindaco, provvederà alla nomina dei responsabili di trattamento nelle persone dei dirigenti e del comandante di Polizia Locale. I responsabili del trattamento possono essere autorizzati dal Titolare alla nomina dei sub-responsabili;
- Il responsabile della protezione dei dati (RPD) oppure DPO (data protection officer), nominato dal Sindaco, ha il compito di:
  a) Informare e fornire consulenza al titolare del trattamento o al responsabile, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal regolamento UE, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal

regolamento UE, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) Sorvegliare l'applicazione del regolamento UE, di altre disposizioni dell'Unione o degli stati membri relative alla protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del regolamento UE 679/2016;
d) Cooperare con il Garante della privacy e fungere da "punto di contatto" con lo stesso Garante per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
e) Verificare la tenuta dei registri del titolare e dei responsabili del trattamento;

TENUTO conto che si è provveduto a:

- effettuare come previsto dal Regolamento UE 2016/679 l'audit per ottemperare al principio di accontability;
- redigere il registro dei trattamenti;
- predisporre le informative previste dalla normativa;
- nominare in data 03/05/2018 con decreto del Sindaco n. 3, il responsabile della protezione (RPD-DPO) nella persona dell'ing. Davide Mario Bariselli di Brescia, per un periodo di due anni;
- predisporre il piano di sicurezza Informatica o GDPR con la relativa documentazione allegata;
- predisporre le "Linee guida sull'uso delle Risorse del Sistema Informativo comunale";

DATO ATTO che nel corso del 2018 si provvederà, altresì:

- Alla nomina dei Responsabili del trattamento dei dati;
- Alla nomina dei sub-responsabili del trattamento dei dati;
- Alla nomina degli incaricati del trattamento dei dati;
- Alla nomina dei Responsabili Esterni del trattamento di dati;
- Ad avviare il registro per l'accesso alla sala server e per gli interventi effettuati dai fornitori sulla rete;
- Ad effettuare corsi di formazione agli incaricati del trattamento dei dati;

VISTO il D.lgs. 267/2000;

VISTO lo Statuto;

VISTO l'allegato parere favorevole in ordine alla regolarità tecnica reso sulla proposta in esame ai sensi dell'art. 49 del D.lgs. 18/08/2000 n. 267;

CON voti favorevoli unanimi, espressi nelle forme di legge

DELIBERA

1) di approvare il "Piano di sicurezza informatica" e gli allegati documenti, allegati al presente provvedimento per formarne parte integrante e sostanziale;

2) di approvare le "Linee guida sull'uso delle Risorse del Sistema Informativo comunale" allegati al presente provvedimento per formarne parte integrante e sostanziale;

3) di dare atto che in data 03/05/2018, decreto n. 3, il Sindaco, in qualità di responsabile del trattamento dei dati, ha adottato il provvedimento di nomina del responsabile della protezione (RPD-DPO) nella persona dell'ing. Davide Mario Bariselli di Brescia, per un periodo di due anni, fino al 31/12/2019;

4) di prendere atto dello stato di attuazione nel Comune di Bellusco del nuovo Regolamento Europeo n .679/2016 sulla protezione dei dati personali evidenziato nelle premesse.

Con separata ed unanime votazione, dichiarare la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134, comma 4, del D.lgs. 18 agosto 2000, n. 267.

_____

Allegati: 1) parere
2) piano di Sicurezza Informatica
3) regolamento Uso del Sistema Informativo
4) allegato 1 Elenco dei Server e dei Software
5) allegato 2 Registro Trattamenti
6) allegato 3 Analisi dei Rischi

DELIBERAZIONE DELLA GIUNTA COMUNALE.

OGGETTO: STATO DI ATTUAZIONE NEL COMUNE DI BELLUSCO DEL NUOVO REGOLAMENTO EUROPEO N.679/2016 SULLA PROTEZIONE DEI DATI PERSONALI.

PARERE DI REGOLARITA' TECNICA

Vista la proposta di deliberazione in oggetto, ai sensi dell'art. 49, comma 1 del D.Lgs. 267/2000, il Responsabile sotto indicato esprime il proprio **parere favorevole** di regolarità tecnica.

IL RESPONSABILE SETTORE AMMINISTRATIVO
Dr. Giorgio Vitali

Letto, approvato e sottoscritto

IL VICE SINDACO
Arch. Mauro Colombo

IL SEGRETARIO COMUNALE
Pepe Dott.ssa Lucia

PUBBLICAZIONE / COMUNICAZIONE

La presente deliberazione è stata PUBBLICATA in data odierna all'Albo Pretorio ove rimarrà esposta per 15 giorni consecutivi.

La stessa sarà esecutiva ad ogni effetto di legge decorsi 10 gg. dalla pubblicazione (art. 134, comma 3, D.Lgs. n. 267/2000).

Addi, 27/07/2018

IL SEGRETARIO COMUNALE
Pepe dott.ssa Lucia

PIANO di SICUREZZA INFORMATICA

GDPR (Generale Data Protection Regulation)

Riferimento al R.UE 679/2016

Comune di Bellusco

(Provincia MB)

Anno 2018

01	25 Mag 2018	Prima emissione del GDPR	Amministratore sistemi Informativi	Titolare del Trattamento
Rev.	Data	Causale	Preparato da	Titolare Trattamento dei Dati

Indice

1 PREMESSA

Il Comune di Bellusco, in qualità di soggetto pubblico, ha predisposto il presente Piano delle Sicurezza del Sistema Informativo (nel seguito denominato più semplicemente PSSI o GDPR) che definisce le policy di sicurezza inerente il sistema di gestione delle informazioni del Comune.
Il piano della sicurezza identifica:

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- gli asset/strumenti utilizzati per il trattamento delle banche dati
- Il Registro dei trattamenti
- l'analisi dei rischi che incombono sui dati (Privacy Impact Assessment);
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- Le attività di formazione relative agli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

Allo scopo di adeguarsi al dettato del Codice, l'Amministrazione comunale ha provveduto ad effettuare un censimento generale delle banche dati sia cartacee che informatizzate contenenti dati personali, distribuite in tutte le sedi del suddetto Ente.

2 CAMPO DI APPLICAZIONE

Il presente documento sulla Sicurezza del Sistema Informativo, si applica a tutti i dati trattati direttamente dal Titolare o, per incarico dello stesso, gestiti all'esterno presso terzi, sia con strumenti elettronici o comunque automatizzati che con altri strumenti e supporti, anche non elettronici.
Esso è l'atto conclusivo di una serie di verifiche sullo stato della "sicurezza informatica" nel comune. La presente procedura si applica alle sedi sotto identificate:

Denominazione Sede	Indirizzo
Sede Municipale	Piazza F.lli Kennedy 1
Biblioteca	Via Corte dei Frati 1

3 CONCETTI, ABBREVIAZIONI, DEFINIZIONI

SW: software

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 struttu-razione, 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.

Dati Personali: 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 identifi-cativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dati Personali Particolari (dati sensibili): dati idonei a rivelare l'origine razziale etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione ai partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati Giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3 comma 1, lettere da a) a o) e da r) a u) del DPR 14 novembre 2002, n 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

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

Incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile

Interessato: persona fisica, l'ente o l'associazione cui si riferiscono i dati personali.

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;

Rischio: con il termine di rischio si identifica l'esposizione alla possibilità di ottenere un guadagno o una perdita economica o finanziaria, di sopportare un danno fisico o un ritardo, come conseguenza dell'incertezza associata al perseguimento di un determinato corso d'azione

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;

Pseudonimizzazione: il trattamento di 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.

"**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

diffusione, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

reti di comunicazione elettronica, i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

rete pubblica di comunicazioni, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

"dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

"dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

"**posta elettronica**", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Vengono di seguito elencate ulteriori definizioni, utilizzate all'interno del presente documento, che possono risultare utili al fine di una maggiore comprensione dello stesso:

"amministratore di rete", soggetto cui è conferito il compito di sovrintendere alla gestione delle risorse fisiche e logiche di una o più reti locali (LAN) ;

"S.I.C.", sistema informatico comunale; l'insieme delle strutture fisiche e logiche (hardware e software) che consentono il trattamento dei dati attraverso apparecchiature informatiche;

"dominio", insieme di utenti e gruppi di utenti attraverso il quale l'Amministratore di rete può gestire diversi aspetti della rete locale tra i quali il più importante è la definizione delle politiche di accesso alle risorse del sistema (es. file, cartelle, stampanti ecc.) ;

"Active Directory", elenco delle risorse presenti in una rete locale che consente, attraverso opportuni strumenti di amministrazione, di gestire le stesse in modo centralizzato;

"utente, user", soggetto che mediante l'utilizzazione di credenziali d'accesso valide può accedere ai servizi di un sistema informatico conformemente ad un profilo per esso definito dall'Amministratore ;

"username", nome identificativo di un utente che, unitamente ad una password, consente l'accesso ad un sistema informatico protetto;

"SID", Security identifier, insieme di numeri di lunghezza variabile il cui valore identifica, in modo univoco, in un sistema windows NT o superiore una risorsa. Tale risorsa può essere un computer un utente o gruppo di essi; se una risorsa viene rimossa e successivamente ricreata con le medesime impostazioni, il SID assegnatogli sarà comunque diverso da quello posseduto precedentemente.

"password", parola chiave che, unitamente ad uno username, consente l'accesso ad un sistema informatico protetto; normalmente viene definita**:**

- **forte** se non è riconducibile all'utente che l'ha generata (nome, cognome, data di nascita, nome della figlia ecc.) e se in caso di attacco di forza bruta è in grado di resistere alla decodifica per un tempo ragionevolmente lungo se paragonato all'attuale sviluppo tecnologico in ambito informatico.

- **debole** se non presenta alcuna delle caratteristiche sopra citate e non consente per questo un accettabile livello di sicurezza.

"attacco di forza bruta (brute force cracking)", viene così definito il tentativo, da parte di persone non autorizzate, di accedere alle risorse di un sistema informatico protetto generando in rapidissima successione credenziali di autenticazione nel tentativo di trovare una combinazione (in genere username e password) valida.

"NTFS", metodo di organizzazione dei dati su un supporto magnetico (file system) che consente di regolare l'accesso ai dati in esso contenuti in base a criteri (permission) definiti dall'Amministratore;

"permission", regola che consente di temperare l'accesso da parte di uno o più utenti o gruppi di essi ad una determinata risorsa (file, cartelle, stampanti ecc);

"policy", politiche di accesso alle risorse di un sistema gestite generalmente a livello centralizzato;

"gruppo di protezione", insieme di utenti utilizzato per gestire gli accessi alle risorse di un sistema informatico centralizzato;

"file sharing", servizio di condivisione file, consiste nella facoltà di un computer di mettere a disposizione di altri utenti del sistema informatico i file in esso contenuti secondo predeterminate policy**;**

"virus informatici", programma in grado di produrre effetti più o meno dannosi a carico di uno o più sistemi informatici interconnessi contro la volontà dei gestori del sistema stesso**;**

"attacco DoS", attacco portato a carico di uno o più computer o dispositivi di rete mirato a provocare il collasso del loro sistema di interconnessione rendendo in tal modo inutilizzabili i servizi dagli stessi erogati.

"TCP/IP", insieme di protocolli che consentono a computer con sistemi operativi anche diversi di dialogare tra loro**;**

"download", trasferimento di dati da un computer remoto ad un computer locale attraverso l'utilizzo di opportuni protocolli di rete;

"sniffing", attività svolta a mezzo di particolari strumenti software e/o hardware che consente di "leggere" i dati in transito in una rete di computer ed eventualmente carpirne informazioni normalmente non accessibili (credenziali d'accesso a sistemi remoti, e-mail, flussi di connessioni ad internet ecc.);

"inconsistenza (dei dati), situazione in cui dei dati, a seguito di un evento doloso o accidentale, non rappresentano più la realtà**;**

"antivirus", software in grado di individuare, bloccare o eliminare virus informatici o codice maligno ed eventualmente riparare i danni dagli stessi provocati;

"definizioni (o firme) dei virus", insieme di informazioni che consentono al software antivirus di riconoscere i virus informatici o eventualmente del codice maligno;

"backup", procedura di salvataggio di dati, può essere eseguita sia su supporti removibili che su computer diversi da quello di origine**;**

"restore", procedura di recupero di dati salvati precedentemente attraverso una procedura di backup**;**

"file di log", file di testo contenente informazioni relative ad un determinato processo normalmente generato dal processo stesso o dal sistema operativo**;**

"standalone", modalità di esecuzione di un software che non implica la presenza di un server o di un'architettura client – server dedicato, viene anche impiegato per indicare un computer non connesso ad alcuna rete locale;

"postazione di lavoro", insieme di strumenti informatici e non normalmente utilizzati da un soggetto per lo svolgimento delle funzioni allo stesso assegnate all'interno della struttura dell'Ente**;**

4 NORMATIVA DI RIFERIMENTO

Le norme e standard di riferimento:

Regolamento Europeo 679/2016 Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

ISO/IES 27001 Information Technology Security Techniques – Code of Practice for information security controls.

Legge 22 aprile 1941, n. 633 e successive modificazioni, Protezione del diritto d'autore e di altri diritti connessi al suo esercizio (G.U. n.166 del 16 luglio 1941) e successive modifiche introdotte dalla L. 18-8-2000 n. 248, "Nuove norme di tutela del diritto di autore." Pubblicata nella Gazzetta Ufficiale 4 settembre 2000, n. 206.

5 ORGANIGRAMMA PRIVACY COMPITI E RESPONSABILITÀ

Le figure identificate dalle disposizioni vigenti in materia di trattamento dei dati sono:

Titolare:
ha potere decisionale in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
Il titolare nomina con contratto o atto giuridicamente valido, il responsabile del trattamento, insieme al quale pone in atto le misure tecniche ed organizzative congrue per garantire un livello di sicurezza adeguato al rischio.

Responsabile Sistemi Informativi:
ha il compito di garantire che il Piano di Sicurezza Informatico venga manutenuto ed aggiornato in funzione dei cambiamenti organizzativi dell'ente, dell'evoluzione degli strumenti usati per il trattamento dei dati
ha il compito di verificare che la policy venga applicata correttamente nell'ambito delle proprie competenze;
ha il compito di promuovere e proporre soluzioni che migliorano la sicurezza del sistema informativo del Comune.
ha il compito di indire periodicamente un incontro per valutare le attività e le proposte dei vari responsabili in materia di sicurezza.

Responsabile trattamento dei dati:
Garantisce la qualità dei dati, le corrette modalità di raccolta, conservazione e trattamento degli stessi, anche da parte del personale della propria struttura, secondo quanto disposto dalla normativa in tema

di trattamento dei dati, dai Provvedimenti del Garante e dal presente documento e vigila sul rispetto delle istruzioni impartite
ha il compito di attuare le politiche di sicurezza nell'ambito del settore di competenza.
ha il compito di suggerire e promuovere azioni che migliorino la sicurezza dei dati trattati dall'ente.
Deve segnalare al DPO l'avvio di nuovi servizi che prevedono il trattamento dei dati
Deve verificare che eventuali fornitori a cui sono affidati il trattamento di banche dati del comune abbiano competenze e modelli di gestione conformi alle indicazioni del nuovo regolamento europeo.

Il DPO (Data Protection Officer)
Ha il compito di:

- rendere noti al Titolare o al Responsabile del Trattamento gli obblighi derivanti dal Regolamento europeo e conservare la documentazione relativa a tale attività di comunicazione o di consulenza;
- vigilare sulla corretta applicazione delle policy in materia di privacy,
- attribuire le responsabilità ad altri soggetti che all'interno dell'ente operano su dati personali;
- vagliare la corretta attuazione delle disposizioni contenute nel regolamento europeo, occupandosi, in particolare di verificare che i sistemi, sin dalla fase della loro progettazione rispettino la privacy (privacy by design) verificare la protezione di default di dati e sistemi (privacy by default), rilevare che venga garantita la sicurezza nei trattamenti dei dati;
- fornire agli interessati un riscontro circa i diritti previsti dal regolamento;
- garantire la conservazione dei documenti relativi ai trattamenti;
- verificare il tracciamento delle violazioni dei dati personali e la loro comunicazione agli interessati;
- verificare che titolare o responsabile effettuino la valutazione dell'impatto delle attività sulla privacy e controllare che venga richiesta l'autorizzazione all'autorità quando occorre;
- fungere da intermediario tra Titolare o Responsabile e autorità Garante in materia di trattamento dei dati;
- controllare che siano rispettati eventuali provvedimenti o richieste espresse dall' autorità Garante in materia di trattamento dei dati.
- elaborazione delle procedure inerenti il trattamento dei dati per le varie attività dell'ente;
- formare il personale in materia di privacy e trattamento dei dati;

5.1 l'Organigramma Inerente il Trattamento dei Dati

Nell' "organizzazione - privacy" dell'ente le figure coinvolte sono:
1. il "Titolare del trattamento": è la "figura" di vertice cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza dei dati.

2. il "Responsabile (interno) del trattamento": è un soggetto designato dal Titolare che, per esperienza, capacità ed affidabilità, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo relativo alla sicurezza. Nell'ambito del comune di Bellusco il Responsabile del trattamento è generalmente individuabile nelle figure apicali, salvo limitate eccezioni. Lo si definisce anche Responsabile "interno" per distinguerlo dal Responsabile "esterno". Relativamente ai trattamenti di dati personali trasversali a più strutture, per l'individuazione si applica il criterio del maggiore ambito decisionale attribuito o vi possono essere situazioni di co-responsabilità.

3. il "Responsabile esterno del trattamento": è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo, esterno all'Amministrazione, che, previa designazione formale del Responsabile "interno" del trattamento, assume (su delega di quest'ultimo) poteri decisionali su un determinato trattamento e deve attenersi, nelle operazioni svolte, alle istruzioni ricevute.

4. l'Amministratore di Sistema: è, in ambito informatico, la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software utilizzati nei vari uffici, le reti locali e gli apparati di sicurezza, nella misura in cui tali attività di gestione e manutenzione consentano di intervenire sui dati personali.

5. l'incaricato del trattamento" (persona autorizzata al trattamento): è la persona fisica che, operando sotto l'autorità del Responsabile, effettua le operazioni di trattamento dei dati, attenendosi alle istruzioni ricevute.

6. il DPO Data Protection Officer: è il soggetto che, coadiuva il Titolare ed il Responsabile del trattamento e gli incaricati nella corretta gestione ed applicazione dei principi definiti dal Regolamento Europeo in termini di data Protection.

7. l'Interessato: è la persona fisica cui si riferiscono i dati personali (sono escluse dal campo di applicazione della normativa privacy le persone giuridiche).

Il Responsabile del trattamento nomina, per iscritto, quali Incaricati del trattamento i propri collaboratori "interni" all'ente. Il Responsabile del trattamento può nominare, per iscritto, quali Incaricati del trattamento, altresì, anche eventuali collaboratori "esterni" dell'Amministrazione (purché persone fisiche), a prescindere dal rapporto contrattuale intrattenuto con la stessa (ad es. stagisti, tirocinanti, ecc.), non dotati di potere decisionale autonomo, se stabilmente presenti negli uffici dell'Amministrazione.

Sanzioni:
il presente documento pone quindi una serie di istruzioni, direttive e linee guida poste a salvaguardia dei dati dei soggetti di cui il comune gestisce i dati, costituenti tutti e ciascuna di essi dati patrimonio

dell'ente stesso. Pertanto, l'eventuale inosservanza o violazione di tali istruzioni, direttive e linee guida costituisce infrazione disciplinare, nonché grave inadempimento ai sensi e per gli effetti dell'art. 1453 del Codice Civile, suscettibile di produrre le conseguenze previste dalla legge, nonché dal contratto collettivo nazionale e individuale di lavoro.

Nell'ambito del Comune di Bellusco vengono identificate le seguenti figure:

Area/Servizio	Posizione Organizzativa Prevista	Ruolo Trattamento dei Dati
Sindaco	Rappresentante Legale	Titolare del trattamento dei dati è il Comune che è rappresentato legalmente dal Sindaco
Procedimenti in carico al segretario	Segretario Comunale	Responsabile Trattamento dei Dati
Area Amministrativa	Responsabile di Area	Responsabile Trattamento dei Dati
Area dei Servizi Economico Finanziari	Responsabile di Area	Responsabile Trattamento dei Dati
Area Educativo e Socio Culturale	Responsabile di Area	Responsabile Trattamento dei Dati
Area Territorio	Responsabile di Area	Responsabile Trattamento dei Dati
Area Polizia Locale Attività Produttive	Responsabile di Area	Responsabile Trattamento dei Dati

6 COMPOSIZIONE DEL DOCUMENTO

Il GDPR identifica le Risorse da Proteggere"; che, in diverso modo, operano o comunque svolgono un ruolo significativo nei processi di trattamento dei dati.

A tal proposito, una volta individuati i dati da proteggere e gli asset utilizzati nella gestione degli stessi, tramite un'altra fase, definita di **Analisi dei Rischi**, sono state valutate e studiate le minacce e le vulnerabilità a cui tali risorse (i dati per l'appunto) sono sottoposte, in modo da potere valutare gli elementi che possono insidiare la protezione, l'integrità e la conservazione di ogni singolo dato personale trattato.

Dall'analisi dei rischi si è redatto un Piano di Sicurezza, tramite il quale si è provveduto a definire l'insieme delle misure fisiche, logiche ed organizzative adottate per tutelare le strutture e le risorse preposte al trattamento dati e quindi ai dati stessi.

Inoltre è stato definito un Piano di Verifiche delle misure adottate tramite il quale si provvederà ad accertare periodicamente la bontà delle misure individuate e ad apportare gli accorgimenti che si riveleranno necessari.

Per completezza, si è ritenuto utile e opportuno allegare al Piano della Sicurezza Informatica una serie di documenti che rendono, con immediatezza, intelligibile a quanti sono coinvolti, a vario titolo, nella politica di protezione e sicurezza dei dati personali adottata dal Titolare, nonché agli organi ispettivi, la politica di protezione e sicurezza dei dati personali (security and data protection policy).

7 REVISIONE DEI DOCUMENTI

L'emissione e la revisione della Piano di Sicurezza del Sistema Informativo, avviene nel rispetto di regole precise e sotto la sorveglianza del Responsabile Area Territorio che garantisce uno sviluppo equilibrato e congruente con l'evoluzione del sistema informativo del Comune.

Le regole da seguire per i vari tipi di documenti sono le seguenti:
Il GDPR contiene le politiche di sicurezza del Comune. Eventuali modifiche della policy e revisioni del documento possono essere suggerite per iscritto da qualsiasi collaboratore dell'ente al Responsabile del Servizio Informativo che le valuta e decide per un'eventuale modifica.

L'analisi dei rischi identifica i possibili eventi indesiderati che possono causare un danno alle risorse del sistema informativo. Una revisione del documento può essere determinata da una serie di motivi, variazione dell'impianto informativo, mutate condizioni organizzative o logistiche.

Le modifiche accolte dal responsabile del Sistema Informativo portano alla revisione del GDPR o della Analisi dei rischi. Va ribadito che l'iter di controllo e approvazione dei documenti, di cui ai punti precedenti, deve rispecchiare quello della prima emissione, a meno di cambiamenti del personale dell'ente o di cambiamenti organizzativi. Per ogni modifica effettuata si aggiorna progressivamente il numero della revisione.
La focalizzazione delle modifiche introdotte con le varie revisioni viene effettuata mediante un segno di evidenziazione del testo. Nel caso di revisione generale, i contenuti della procedura variati sono tali da considerarne una nuova impostazione.
L'aggiornamento dell'archivio cartaceo e di quello elettronico, relativi al PSSI, è compito del Responsabile del sistema informativo.
Quando un Documento della sicurezza è revisionato, Responsabile del Sistema Informativo, conserva la copia superata in formato elettronico in un'apposita directory denominata "Doc_Sicurezza_Superati".

Documento	Redazione	Approvazione	Distribuzione	Archiviazione
PSSI/GDPR	Amministratore di Sistema	Titolare	Responsabile Segreteria	Responsabile Segreteria
Procedure	Amministratore di Sistema	Titolare	Responsabile Segreteria	Responsabile Segreteria
Regolamento Utilizzo Risorse Sistema Informativo	Amministratore di Sistema	Titolare	Responsabile Segreteria	Responsabile Segreteria

8 IDENTIFICAZIONE DELLE RISORSE E DELLE INFRASTRUTTURE

Le risorse che in qualche modo intervengono nel trattamento dei dati del titolare sono identificate da:

- Luoghi fisici
- Banche dati
- Apparecchiature
- Personale

Di seguito verrà data una descrizione sommaria di questi elementi.

8.1 Luoghi Fisici

I luoghi fisici dove si svolge il trattamento dei dati sono identificati nel paragrafo capitolo 5

8.2 Sistema Informativo

8.2.1 Server e risorse elaborative

Il sistema informativo del comune di Bellusco si compone di una serie di server installati all'interno di locali con accesso selezionato al piano terra della sede Comunale.
Sui server sono installate gli applicativi di gestione dei vari uffici e vengono salvati i file di produttività individuale usati dai vari uffici; L'accesso alle banche dati avviene tramite Rete Locale.
Nella tabella allegata al piano sono identificati i server, il sistema operativo installato e le banche dati presenti sul server e le soluzioni di sicurezza adottate.

8.2.2 Networking

La rete LAN è una rete basata su sistema operativo Microsoft.
L'infrastruttura di rete del comune è costituita da una sala ced, ubicata nell'edificio principale del comune, in cui sono installati i server del SIC.
Nella tabella allegato1 al presente pino sono identificati i server, il sistema operativo installato e i servizi applicativi e le banche dati presenti sul server.
Nella tabella riportata nell'Allegato 1 sono identificati gli apparati principali della SIC.
Di seguito viene descritta l'infrastruttura di rete del comune

Infrastruttura di rete
Connessione alla rete Internet
Il collegamento alla rete internet è gestito da un provider tramite un collegamento in fibra e linea di backup ADSL
Apparati di protezione Perimetrale
La rete della sede centrale è protetta da un router che fa da firewall
Sala CED
Nella sala ced sono installati gli switch del centro stella che sono collegati con gli armati di rete dislocati ai vari piani Gli apparati di rete del centro stella sono alimentati con batterie di continuità
Apparati di rete ai piani
Ai vari piani degli edifici del comune possono essere presenti degli armadi di rete nel quale sono installati gli apparati di connettività che collegano le postazioni di lavoro

8.2.3 Personal Computer

I PC in dotazione ai collaboratori del comune sono dotati di sistemi operativi windows. Su ogni di essi è installato l'antivirus che viene periodicamente aggiornato.
L'accesso alle risorse di rete avviene tramite account composto da un identificativo e da una password.
Su ogni computer è installato un software antivirus che viene gestito da una console centrale che consente di monitorare la sicurezza delle postazioni di lavoro.
Il software consente anche di identificare eventuali problemi di aggiornamento dell'antivirus.

8.2.4 Risorse Software

Gli applicativi software utilizzati per il trattamento dei dati sono descritti nell'Allegato 1

8.3 Registro dei Trattamenti

Gli applicativi software utilizzati per il trattamento dei dati sono descritti nell'Allegato 2

9 ANALISI DEI RISCHI

I rischi a cui un sistema è sottoposto possono derivare dall'interno o dall'esterno, essere accidentali o volontari. Questi possono causare la perdita delle informazioni, la loro alterazione, o la non disponibilità.

Tra i possibili fattori di rischio del sistema rientrano:

- Calamità naturali
- Accesso non autorizzato
- Diffusione di software maligno
- Errori nel codice del sw
- Errori nella trasmissione dei dati
- Furti
- Errori umani
- Guasti alle apparecchiature

Una volta identificati i possibili fattori di rischio associato alle diverse parti del Sistema Informatico (asset) è stata descritta la vulnerabilità ed il rischio ad essa associata.
Questo passaggio ha lo scopo di inquadrare i danni che potrebbero essere arrecati alle risorse del sistema.

L'analisi dei rischi è fondamentale per la identificazione le strategie da attuare per prevenire o ridurre il danno.
Un aspetto nell'analisi dei rischi consiste nello stimare le probabilità di accadimento degli eventi indesiderati (dimensione probabilistica).
Questa valutazione è stata fatta dal team di progetto in funzione dell'esperienza delle persone che hanno condotto l'analisi e in relazione alle conoscenze dell'ambiente e del sistema informativo del comune e tenendo conto delle contromisure adottate dall'ente per mitigare il rischio.

L'ultimo step per la quantificazione del rischio, consiste nel valutare la gravità che questi eventi accidentali possono causare, attuare degli interventi per migliorare la sicurezza del sistema che sono stati riportati nella tabella seguente.
Nel contesto del progetto, la stima degli inconvenienti causata dal verificarsi di certi eventi, non è stata fatta usando un criterio economico. Questo perchè molti dei danni che si possono riscontrare sono difficili da quantificare, in quanto legati a disservizi causati ai cittadini o alla perdita di immagine del Comune. Anche in questo caso si è preferito identificare le priorità degli interventi da attuare in base all'esperienza del team di progetto e in funzione delle scelte economico/strategiche dell'ente.

9.1 RISULTATI DELL'ANALISI

Il registro dei trattamenti descrive le banche dati gestite dal titolare e dai responsabili, ed è riportato nell'Allegato 3
Oltre alle banche dati sono anche identificati i soggetti a cui i dati vengono comunicati, siano essi enti Pubblici o aziende che per conto del comune svolgono un servizio.

10 PIANO DI SICUREZZA

10.1 Misure organizzative

10.1.1 Nomina del personale incaricato al trattamento dei dati

Nell'ambito del Comune di Bellusco sono adottati una serie di procedimenti organizzativi volti a migliorare la sicurezza del sistema informativo.
Innanzitutto sono state identificati i ruoli e le responsabilità delle figure professionali che nell'ambito dell'ente trattano dati.
Le figure professionali identificate sono state formalmente incaricate attraverso una delega scritta che identifica competenze e responsabilità relative alla gestione del sistema informativo e al trattamento dei dati.

Le regole di nomina prevedono:

1. Il Titolare Nomina i Responsabili Interni del trattamento dei dati
2. I responsabili Interni incaricano i soggetti che trattano i dati
3. I Responsabili interni nominano i responsabili esterni - fornitori (soggetti che per conto del comune svolgono servizi che prevedono il trattamento dei dati)

Le strutture all'interno dell'organizzazione complessiva del Comune che si occupano del trattamento di dati personali, anche in relazione ai compiti loro assegnati, sono state individuate in base alla tipologia, all'entità, alla distribuzione e alla organizzazione delle attività svolte all'interno dell'ente.
A tale scopo ciascun dipendente e collaboratore è incaricato ed autorizzato al trattamento dei diversi tipi di dati; gli incarichi - così come la responsabilità per la conservazione dei dati vengono conferiti personalmente al momento dell'inserimento di una nuova figura all'interno della struttura dell'ente;
ciascun incaricato può operare, per il trattamento dei dati, esclusivamente all'interno delle mansioni assegnate e in riferimento alle informazioni ed alle Banche dati disponibili relative alla propria categoria di appartenenza;

Lavoratori a tempo determinato/stagisti/ LSU: i soggetti che trattano dati riferiti all'attività del Comune che, per qualifica attribuita od in relazione alla concreta attività svolta, non rivestono la figura di incaricati, sono stati opportunamente autorizzati al trattamento mediante specifica Nomina (stagisti ecc.).

10.1.2 Regole accesso Organi politici e consigliari ai dati trattati

Per quanto riguarda il Consiglio Comunale e la Giunta; tali organi non hanno ruoli diretti di gestione delle banche dati, tuttavia, al fine di svolgere appieno il mandato loro conferito, il sindaco, gli assessori e i consiglieri possono consultare ogni documento, sia cartaceo che informatico, anche contenente dati sensibili;

10.1.3 Aziende addette alla Manutenzione degli strumenti di Elaborazione, dei software e delle reti informatiche

Nel caso in cui l'ente richieda l'intervento di ditte specializzate per interventi di assistenza e manutenzione, questi soggetti operano in base a specifica autorizzazione, recante nel dettaglio i compiti da svolgere. In particolare queste Ditte si trovano nella situazione di dover periodicamente svolgere lavori di manutenzione o, semplicemente, di verifica del funzionamento di un programma o di una attrezzatura informatica. A tal fine è praticamente necessario accedere alle banche dati presenti sui personal computer o all'interno dei programmi software, che si configura come un trattamento ed una conoscenza di dati personali che di per sé non è collegata allo scopo per cui la Ditta effettua la propria attività.
Se l'adozione delle misure di sicurezza viene affidata a soggetti esterni alla propria struttura, quali i fornitori di programmi software dedicati, il Titolare del trattamento riceve dall'installatore una descrizione scritta dell'intervento effettuato e delle operazioni realizzate.

10.2 Audit sulla corretta attuazione dei principi e delle regole di trattamento dei dati

E' stato predisposto un piano di audit per verificare periodicamente la corretta attuazione dei principi e delle misure organizzative e tecniche inerenti il trattamento dei dati e per rivedere l'analisi dei rischi ed il piano delle azioni da implementare per un miglioramento dei processi di gestione delle informazioni. Una sintesi delle attività previste è riportata nel **capitolo 17** del presente documento.
Gli audit sulla compliance al REU 679/2016 sono svolti dal DPO in collaborazione con i Responsabili del trattamento dei dati e con l'amministratore di sistema. Al termine di questa attività viene prodotta una relazione nella quale vengono evidenziati i piani e le attività di miglioramento che il comune deve adottare (Rapporto di Audit)

10.3 Gestione profili di autorizzazione di accesso al sistema informativo

Nel caso di nuova assunzione o nel caso di variazione dell'organico la procedura (PO-PSI-01) definisce le regole di gestione degli utenti del sistema informativo. La policy prevede la comunicazione, da parte del responsabile dell'area presso la quale il dipendente presta/presterà servizio all'amministratore di sistema, delle variazioni delle mansioni e dei nuovi profili di accesso alle risorse del sistema informativo comunale.
L'amministratore di sistema incaricato dovrà modificare i diritti di accesso alle risorse del sistema informativo e ai dati trattati attraverso strumenti informatici.

10.4 Gestione e comunicazione dell'Informativa

Come previsto dal RE 679/2016 il comune di Bellusco ha predisposto dei modelli di informativa rivolti alle diverse categorie di soggetti interessati:

- Cittadini
- Dipendenti del comune
- Professionisti e dipendenti dei Fornitori

L'informativa è stata esposta, presso i vari uffici e gli sportelli a cui il pubblico accede abitualmente.

Per il settore dei servizi sociali, quando si attiva un procedimento che prevede il trattamento di dati relativi allo stato di salute, il documento di informativa viene consegnato al soggetto interessato ed una copia controfirmata viene archiviata nella pratica.
Una comunicazione relativa alle regole e alle modalità di trattamento dei dati è stata esposta sul sito del comune alla sessione Privacy.
La procedura PO-PSI-04 definisce le regole e le modalità di gestione dell'Informativa e delle modalità con cui acquisire il consenso al trattamento dei dati.

10.5 Gestione delle Comunicazioni e della Pubblicità legale attraverso sito web e l'albo pretorio

La legge n. 69 del 18 giugno 2009, perseguendo l'obiettivo di modernizzare l'azione amministrativa mediante il ricorso agli strumenti informatici riconosce l'effetto di pubblicità legale agli atti e ai provvedimenti amministrativi pubblicati dagli Enti Pubblici sui propri siti informatici.

10.5.1 Pubblicazione on line e rispetto della privacy

Le regole sulla privacy dettate nel Decreto Legislativo n.196 del 2003, che garantiscono il diritto alla tutela dei dati personali sono valide e debbono essere rispettate anche per i siti web (per es. dagli atti pubblicati vanno omessi i dati sensibili ossia quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale)
L'albo pretorio contiene diversi provvedimenti che devono essere pubblicati per legge e che possono, a volte, fare menzione di alcuni dati sensibili strettamente indispensabili. Nel predisporre i documenti da affiggere, però, fermo restando il rispetto degli obblighi di legge sulla trasparenza delle deliberazioni adottate, occorre comunque rispettare la riservatezza degli interessati. La pubblicazione indiscriminata di informazioni personali può porsi, infatti, in contrasto con la legge sulla privacy quando ciò non sia necessario al raggiungimento delle finalità per le quali i dati sono stati raccolti.
Con la delibera n.17 del 19 aprile 2007 Allegato1 - Internet: sui siti di comuni e province trasparenza, ma con dati personali indispensabili – Allegato 1: Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali - il garante della privacy consente la diffusione di dati personali per finalità di trasparenza e di comunicazione nelle pubbliche Amministrazioni ma sempre nel rispetto dei principi di pertinenza, non eccedenza e indispensabilità dei dati da pubblicare su internet e pone nuovamente cautele e limiti di fronte alla pubblicazione di dati sensibili che inoltre, richiedono l'adozione di misure di sicurezza per garantire il trattamento dei dati con strumenti elettronici.

10.6 Sicurezza Fisica

La politica della sicurezza identifica i comportamenti che regolano l'accesso fisico a luoghi in cui sono conservati o custoditi dati personali o sensibili. A tale proposito si può identificare una classificazione degli stessi in:

- Aree ad accesso non controllato
- Aree ad accesso controllato

- Aree ad accesso ristretto

Per ognuna di queste sono state definite delle modalità di gestione degli accessi e delle regole per quanto riguarda l'installazione delle apparecchiature.

10.6.1 Controllo degli accessi agli edifici

Le sedi del comune in cui viene effettuato il trattamento dei dati sono identificate nel capitolo 2 del presente PSSI. Nella tabella sottostante vengono identificati i sistemi di controllo degli accessi ai vari edifici e gli impianti di sicurezza installati

Sede 1	**Sede Municipale**
Indirizzo	Piazza F.lli Kennedy 1
Portierato	No
Video sorveglianza	Perimetrale
Allarme antintrusione	Si, sensori di movimento Attivazione e Disattivazione in automatico 20:30/06:30 Collegato cell. Sindaco , arch. Bettini, Carabinieri
Inferriate	No , Presenti Tapparelle
Vigilanza notturna	No
Antincendio	Estintori
Accesso all'edificio descrivere	Portone in ferro
Accesso all'edificio descrivere	Seconda porta in alluminio e vetro
Distribuzione chiavi registrata	I dipendenti accedono dalla porta di servizio con badge

Sede 2	**Polizia Locale**
Indirizzo	Via Ornago 24
Portierato	no
Video sorveglianza	No
Allarme antintrusione	si
Inferriate	no
Vigilanza notturna	no
Antincendio	Si tramite estintori
Accesso all'edificio descrivere	Accesso principale porta a vetri e alluminio
Accesso all'edificio descrivere	Accesso secondario porta a vetri e alluminio
Distribuzione chiavi registrata	Accesso da parte del personale del comando a cui sono state distribuite chiavi e codici di accesso

Sede 3	**Biblioteca**
Indirizzo	via Corte dei frati 1
Portierato	No
Video sorveglianza	No

Allarme antintrusione	Si, sensori di movimento Attivazione e Disattivazione in automatico Collegato cell. Sindaco , arch. Bettini, Carabinieri
Inferriate	No
Vigilanza notturna	No
Antincendio	Rilevatori di fumo ed estintori
Distribuzione chiavi registrata	Personale della Biblioteca, ufficio tecnico, Impresa Pulizie

10.6.2 Aree ad accesso non controllato

Sono quelle aree in cui il pubblico può accedere senza alcuna identificazione o misura di sicurezza. Rientrano in questa categoria:

- la sala del consiglio
- la sala riunioni
- sala assessori

Regole relative a questi spazi

In queste aree non devono essere installate apparecchiature informatiche contenenti banche dati; non devono essere presenti apparecchiature collegate alla rete del comune, se le stesse non sono presidiate da un operatore;
non devono essere presenti archivi documentali non adeguatamente protetti.

10.6.3 Aree ad accesso controllato

Sono quelle aree in cui può accedere solamente il personale dipendente dell'ente, nel caso in cui acceda del personale esterno questo deve essere accompagnato da un collaboratore del comune. In questa tipologia rientrano anche le aree accessibili liberamente al pubblico che durante l'orario di apertura devono essere presidiate dai collaboratori del Comune. Rientrano in queste spazi:
Uffici del comune
Uffici di sportello

Regole relative a questi spazi

Queste aree/uffici al termine dell'orario di lavoro o di chiusura degli sportelli devono essere chiuse al pubblico.
In queste aree possono essere installate apparecchiature informatiche collegate alla rete interna.
Le stazioni di lavoro devono rispettare una serie di misure minime di sicurezza:

- accesso alle risorse del Sistema Informatico attraverso password conosciuta unicamente dall'operatore;
- eventuali apparati di rete devono essere disposti in armadi chiusi.
- gli archivi contenenti banche dati su supporto cartaceo devono essere chiusi a chiave, nel caso siano ubicati nelle aree di permanenza del pubblico.

10.6.4 Aree ad accesso ristretto

Sono quelle aree in cui sono installate apparecchiature critiche quali server, apparati di rete, nonché documenti e banche dati cartacee. L'accesso a tali aree è consentito solamente al personale autorizzato e devono essere all'interno di edifici sotto la responsabilità dell'Amministrazione Comunale.
I locali devono rimanere chiusi e le chiavi custodite dalle persone autorizzate.
L'accesso del personale esterno è regolamentato dal Responsabile.
Le aree ad accesso ristretto identificate presso il Comune di Bellusco sono essenzialmente:

- la Sala Server
- l'Archivio di Deposito e Storico

Regole di accesso SALA SERVER

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi. Le misure riguardano la sala server del comune accessibile attraverso una porta dotata di serratura la cui chiave è in dotazione al responsabile dei sistemi informativi e all'elettricista del comune.
Un'ulteriore copia delle chiavi è custodita dal responsabile dell'Ufficio Tecnico nel caso si debba accedere alla sala per motivi di emergenza in orari di chiusura degli uffici.

Sala Server	Regole Sicurezza
Serratura	Serratura con chiave di sicurezza
Distribuzione chiavi	Responsabile Sistemi Informativi - Lavori Pubblici - Affari Generali
Registro accesso	Non Impiegato
Allarme accesso	Non attivo
Antincendio	Estintori a CO2 in prossimità
Impianto energia elettrica a norma	Si periodicamente vengono fatti i controlli della messa a terra
Aria condizionata per raffreddamento delle apparecchiature	Nella sala ced è presente impianto aria condizionata
Installazione sistemi UPS	Gli apparati di rete ed i server sono alimentati da batterie di continuità

Accesso da parte del personale esterno

Il personale non dipendente che deve accedere al comune per la manutenzione degli apparati, degli applicativi software o degli impianti, deve registrare l'attività svolta sul registro di controllo degli accessi, indicando le proprie generalità, data di ingresso, data di uscita.
Quando delle persone entrano nella Sala server il loro operato è supervisionato da un collaboratore dell'ufficio informatico, che si preoccupa anche di impartire indicazioni inerenti le regole di accesso ai locali.

Nella tabella sottostante sono identificate le misure di protezione fisica della sala server e della sala macchine ubicate nei vari edifici nelle quali sono presenti apparati critici del sistema informativo dell'ente.

Regole di Accesso all'Archivio Comunale storico o di deposito

L'archivio del comune si distingue in archivio corrente, ed archivio storico.
L'archivio corrente è identificato nelle scaffalature e negli armadi degli uffici del comune, per i quali verranno identificate delle regole di accesso opportune.
L'archivio storico contiene dati e documenti, ed è ubicato in un locale del comune a cui possono accedere solamente le persone autorizzate.
L'accesso all'archivio è consentito solo al personale autorizzato, richiedendo la chiave all'ufficio protocollo. E' stato inoltre predisposto un registro M-PSI-21 in cui si devono identificare i documenti prelevati.

Archivio Documentale	Regole Sicurezza
Distribuzione chiavi	Ufficio Segreteria e Lavori pubblici
Registro accesso	Impiegato
Allarme accesso	Allarme di zona Non attivo - Allarme generale dell'Edificio
Antincendio	Estintori
Impianto energia elettrica a norma	Si periodicamente vengono fatti i controlli della messa a terra

10.6.5 Facility dell'edificio

Di seguito vengono identificate le misure adottate per la gestione della sicurezza e per la prevenzione di eventi naturali dannosi.

Impianto elettrico

L'impianto rispetta la normativa vigente. Eventuali interventi vengono svolti da ditte specializzate.
Periodicamente l'ufficio manutenzione fa un controllo della messa a terra dell'edificio.

Numeri telefonici di emergenza

I numeri telefonici delle ditte che curano l'assistenza hardware e software sono riportati in un elenco appeso nel locale ove sono custoditi il server di rete.

11 REGOLE DI MISURE DI SICUREZZA

In questo paragrafo vengono identificate le politiche per la gestione logica della sicurezza delle informazioni che interessano quindi l'accesso alle basi di dati attraverso gli apparati del sistema informativo.

11.1 Identificazione utenti del sistema informativo

Ogni utente può accedere alla rete del sistema informativo attraverso un identificativo (user id) univoco e password. L'identificativo e la password sono personali in modo che non sia possibile accedere da due postazioni di lavoro con lo stesso identificativo.
L'assegnazione dei diritti di accesso alla rete informatica o alla base di dati viene fatta dal responsabile del sistema informativo previa richiesta fatta dal responsabile del trattamento dei dati

11.1.1 Password

La password è assegnata a ciascun utente in forma riservata. Allo stesso è consentito di variarla. La gestione della password prevede una serie di misure sotto riportate atte a rendere efficace l'utilizzo della stessa:
lunghezza minima 8 caratteri;
deve essere sostituita ogni 3 mesi;
non deve essere simile alla precedente;
non deve essere comunicata ai colleghi;
non deve essere annotata su supporti accessibili o leggibili;
non deve contenere termini facilmente riconducibili all'incaricato.

11.1.2 Autenticazione degli utenti

Il sistema informativo prevede due livelli di autenticazione:
autenticazione per accesso alle risorse del sistema. Il Comune di Bellusco , utilizza i servizi di autenticazione del sistema operativo windows che prevedono la definizione della lunghezza minima delle password a 8 caratteri e l'utilizzo di una complessità nella definizione del codice di autenticazione.
autenticazione applicativa. Per quanto riguarda gli accessi agli applicativi di business, sono state fornite precise istruzioni ai collaboratori sulla necessità di variare la password secondo le regole sopra indicate. Inoltre, per quelle soluzioni la cui gestione viene fatta da enti esterni, si deve prevedere la comunicazione della stessa all'amministratore delle password come evidenziato nella tabella di seguito riportata.

11.1.3 Gestione Utenze amministrative

Nell'ambito della gestione della rete del comune sono state identificati dei soggetti che si occupano della gestione del sistema informativo (amministratori di sistema)
A questi soggetti sono assegnate credenziali di amministratore che devono essere gestite secondo quanto definito nella circolare AGID n 2-2017.
Le policy di gestione sono le seguenti:

Policy gestione utenze Amministrative	
Identificativo	L'identificativo dell'utenza amministrativa deve fare riferimento ad una persona
Password	La password deve essere di 14 caratteri (rif circolare AGID 2 /2017)
Complessità della Password	La gestione delle parole chiave deve prevedere delle regole di complessità -scadenza ogni tre mesi e non riutilizzo per 3 volte di seguito (rif circolare AGID 2 /2017)
Conservazione delle parole chiave	Le parole chiave devono essere custodite in un luogo sicuro a disposizione del titolare e del responsabile del sistema informativo

11.1.3.1.1 Gestione delle utenze amministrative di soggetti esterni

La gestione del sistema informativo comunale vede la presenza di soggetti esterni quali i fornitori delle applicazioni software usate dagli uffici, soggetti che intervengono nella gestione della rete ecc che per operare devono disporre di utenze amministrative.
La gestione di queste utenze è in carico all'amministratore di sistema del comune che ha il compito di adottare le seguenti policy:

Policy gestione utenze Amministrative di soggetti esterni	
Permessi	Ad ogni soggetto deve essere assegnata una utenza amministrativa univoca i cui permessi sono limitati all'attività che lo stesso deve svolgere
Identificativo	L'identificativo dell'utenza amministrativa deve fare riferimento ad una persona
Password	La password deve essere di 14 caratteri
Complessità della Password	La gestione delle parole chiave deve prevedere delle regole di complessità
Conservazione delle parole chiave	I soggetti a cui sono assegnate queste utenze amministrative sono registrati in un file a disposizione dell'amministratore interno. Questo consente di tenere traccia dei soggetti a cui sono assegnate e di verificarne l'utilizzo

Le politiche di sicurezza sono descritte nella PO-PSI-01 Gestione utenti del Sistema Informativo

11.1.4 Le regole di autenticazione alla rete del comune

La gestione dell'assegnazione dei diritti di accesso viene fatta dall'amministratore di Sistema. Nel caso un collaboratore del comune si dimetta i diritti di accesso devono essere revocati attraverso una comunicazione all'amministratore del sistema da parte dell'ufficio del personale del Comune di Bellusco. Id e password utilizzate non possono essere associate ad un altro utente.

Variazione incarico

Nel caso in cui il collaboratore ricopra un incarico diverso deve essere fatta una comunicazione al responsabile del sistema informativo il quale provvede a modificare i permessi di accesso alle banche dati e alle risorse del sistema informativo.
La richiesta, deve essere fatta in forma scritta all'Amministratore di Sistema da parte del Responsabile dell'Ufficio che accoglie il dipendente.

Nel caso un'utente del comune si assenti per un determinato periodo di tempo, il responsabile dei sistemi informativi è in grado di cancellare la password impostata dall'utente e di creare un nuovo id in modo da poter accedere alle risorse del PC.
In modo analogo l'amministratore del sistema è in grado di creare degli utenti temporanei per accedere agli applicativi di business. Per cui la comunicazione delle password in busta chiusa seguirà le regole definite nella PO-PSI-01.

11.1.5 Comunicazione di variazione delle password

Per quegli applicativi e strumenti elettronici il cui accesso è consentito esclusivamente tramite credenziali di autenticazione, la cui gestione e variazione non è riconducibile all'ufficio informatico, la stessa deve essere gestita in forma controllata.
In ogni settore viene identificato un responsabile delle password che gestisce attraverso un registro elettronico o documentale l'elenco dei servizi applicativi esterni al comune
Nel caso di assenza prolungata dell'incaricato del trattamento dei dati il responsabile dei sistemi informativi o un collaboratore del comune, previa autorizzazione del responsabile del trattamento, possono utilizzare le credenziali di autenticazione avvertendo l'incaricato dell'intervento effettuato.

11.2 Gestione degli Archivi documentali

Il comune di Bellusco gestisce archivi documentali contenenti sia dati personali che sensibili che giudiziari.
Per quanto riguarda la gestione degli archivi cartacei l'ente ha adottato le seguenti regole:
nel caso di documenti archiviati in armadi collocati in luoghi non presidiati dai dipendenti ed accessibili al pubblico, questi devono essere chiusi a chiave in modo da garantire la privacy e l'integrità delle informazioni contenute.
dati personali archiviati in armadi dei vari uffici sono chiusi a chiave, nel caso ciò non sia possibile si provvede a chiudere a chiave l'ufficio.

I **dati sensibili e giudiziari** necessariamente vanno custoditi in armadi dotati di serratura chiudibile a chiave.
Se durante le ore di lavoro, l'operatore del Comune deve accedere ai documenti cartacei contenenti dati relativi ai cittadini del Comune o dati relativi alla gestione dell'ente, gli stessi devono essere gestiti con attenzione in modo da non pregiudicarne la privacy o la sottrazione indebita. Al termine della consultazione gli stessi devono essere riposti con cura negli armadi da cui sono stati prelevati.

Nel caso alcuni documenti contenenti dati personali, sensibili o dati classificati come importanti non siano più utili questi devono essere distrutti in modo da non risultare leggibili.
La gestione dei documenti cartacei compete ai responsabili del trattamento dei dati ognuno per le proprie competenze.

11.2.1 Regole chiusura Uffici ed Armadi

Uffici

- al termine dell'orario di lavoro gli uffici devono essere chiusi; le chiavi sono in possesso ad almeno due persone dell'ufficio ed una depositata presso ufficio manutenzioni.

Armadi (nel caso in cui gli uffici non siano chiudibili): al termine della giornata lavorativa i documenti contenenti dati sensibili vanno riposti negli armadi che devono essere chiusi. Le chiavi sono depositate in un armadio chiuso, la cui chiave viene custodita secondo le disposizioni del Responsabile dell'ufficio.

11.2.2 Gestione della comunicazione dei dati tramite documenti Cartacei

In questo paragrafo vengono identificate le regole per la trasmissione dei documenti cartacei nell'ambito del Comune di Bellusco.

Le regole adottate dall'ente prevedono:
le comunicazioni in ingresso vengono protocollate dall'ufficio del protocollo, e i documenti classificati come riservati o contenenti dati sensibili vengono registrati e inoltrati all'ufficio competente come riservati;
nel caso di comunicazioni verso l'esterno, la protocollazione della posta è gestita dai singoli uffici.

Per la trasmissione di documenti tra uffici del Comune, compresi lo smistamento della posta da parte del protocollo, deve rispettare una serie di principi in particolare quello di necessità e pertinenza. Cioè i dati possono circolare solo per ragioni di servizio e per la necessità dei singoli uffici; inoltre la corrispondenza non deve passare indiscriminatamente da più persone evitando passaggi superflui.

11.3 Sicurezza della rete informatica

11.3.1 Attacchi alla sicurezza Informatica

Senza la pretesa di offrire una classificazione formale e completa, possiamo considerare gli attacchi come violazioni delle proprietà di sicurezza precedentemente enunciate. I tipi di attacchi possono essere dunque:

- intercettazioni (violano la proprietà di segretezza dell'informazione);
- alterazioni (violano il requisito di integrità);
- generazioni (violano i requisiti di autenticità e di non-ripudio);
- interruzioni (minacciano la disponibilità del sistema).

Nella tabella sono elencate le caratteristiche principali di ogni categoria di attacco, insieme ad alcuni esempi presi da contesti reali.

11.3.2 Sicurezza della rete

La rete consente alle varie stazioni di lavoro di collegarsi alle unità centrali di elaborazione dei dati. Una rete locale mediante opportuni apparati si può poi collegare ad internet, è intuitivo che i livelli di protezione del sistema informativo cambiano se si verifica quest'ultima condizione.

La rete del comune di BELLUSCO è configurata mediate la definizione di un **Dominio di rete** a cui accedono gli utenti previa autenticazione. Per quanto riguarda la rete locale la politica di gestione degli indirizzamenti prevede l'utilizzo di uno schema di indirizzi IP che utilizzano il servizio DHCP.

Nela tabella di seguito riportata vengono descritte le misure di sicurezza informatica adottate dal comune

Gestione Sicurezza della rete	
Collegamenti internet	Collegamento linea ADSL con linea di backup Telecom
Strumenti di Protezione perimetrale: Firewall	la rete del comune è protetta da router che fa da firewall
Strumenti di Protezione perimetrale: IPS	No
Strumenti di Protezione perimetrale: Antivirus	no
Strumenti di Protezione perimetrale: Antispam	Fornito dal provider che offre il servizio di posta
Proxy	Non presente
Viene fatta copia del domain controller	si
Regole aggiornamento sistema operativo server	gestito in automatico
Configurazione ed installazioni delle Postazioni di lavoro e Server	
Aggiornamento dei sistemi operativi	SERVER: Gli aggiornamenti delle macchine server vengono fatti in base all'importanza e alla criticità della Patch. L'infrastruttura in cui sono installati i software di gestione dei vari uffici sono gestite dal fornitore del servizio di assistenza sistemistica PDL: sulle postazioni di lavoro è attivo il servizio di aggiornamento in automatico del sistema operativo
Viene tenuta traccia delle attività di eventuali interventi di manutenzione dei server di rete?	Gli interventi di installazione o manutenzione della rete informatica sono tracciati con dei rapportini di intervento che specificano le attività realizzate da parte di ditte esterne

L'installazione delle postazioni di lavoro viene fatta usando una procedura definita che identifica configurazioni e strumenti di sicurezza da attivare ?	L'installazione delle postazioni di lavoro viene fatta installando un set predefinito di applicazioni software e tool di sicurezza
Sono state attivate configurazioni che consentono il ripristino delle Pdl	Nel caso di cattivo funzionamento di una PDL viene fatta reinstallazione - Sui computer con sistema operativo W10 è attiva la funzione di ripristino del sistema informativo
tool di protezione delle PdL e dei Server	
L'antivirus ha una console di gestione centralizzata che consente di impostare le regole di sicurezza	Antivirus
Il sw antivirus controlla la presenza di codice maligno quando si collega un dispositivo esterno ?	controllo dispositivi esterni quando viene collegato al PC
Regole controllo codice maligno	Controllo in tempo reale, programmazione scansione completa del PC impostato durante pausa pranzo
Antivirus controlla se sulla Pdl Vengono installati applicazioni non autorizzate	Funzione non presente
Il fornitore del servizio di posta ha attivato un Servizio Antispam	si
Sulle postazioni di lavoro è stato attivato il Firewall personale	si

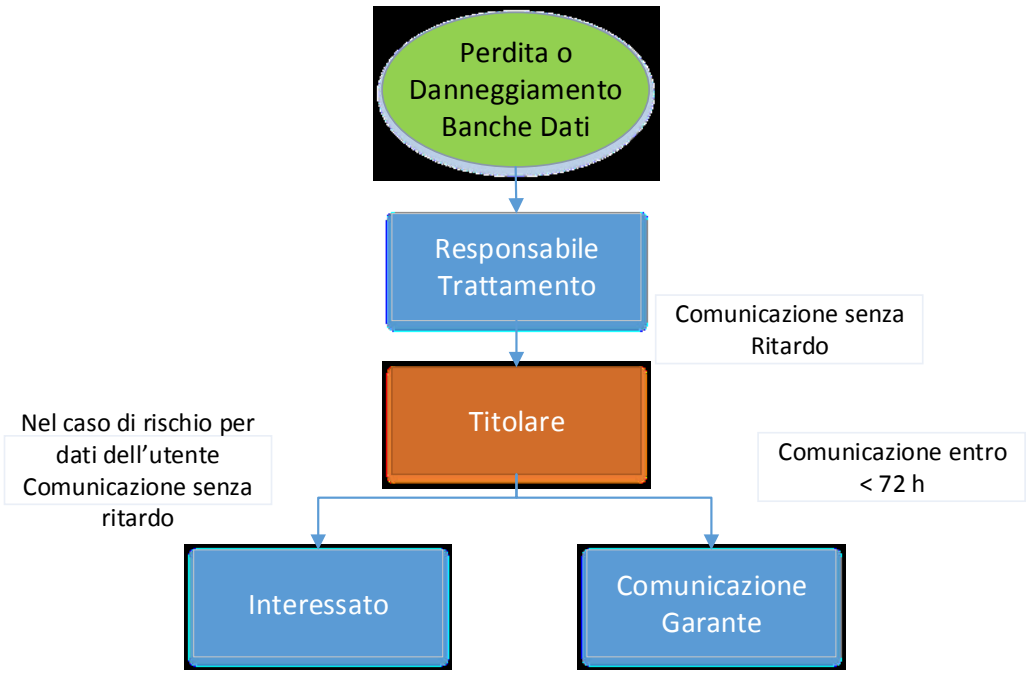
12 VIOLAZIONE O PERDITA DEI DATI

Nel caso in cui ci sia una violazione dei dati personali, intesa come la "violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ad informazioni personali trasmesse, memorizzate o comunque trattate, l'ente è tenuto a darne comunicazione all'autorità competente.
Entro 72 ore dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante (tramite apposito modello Allegato1 pubblicato sul sito www.garanteprivacy.it) tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali.

La comunicazione deve:

1. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. identificare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
3. descrivere le probabili conseguenze della violazione dei dati personali;
4. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Inoltre, quando la violazione dei dati personali è suscettibile di danno per i diritti e le libertà delle persone fisiche, il Titolare deve comunicare la violazione anche all'interessato, senza ingiustificato ritardo, descrivendola con un linguaggio semplice e chiaro (salve circostanze al verificarsi delle quali la comunicazione è esclusa).



13 FORMAZIONE

La gestione della sicurezza informatica in una qualsiasi organizzazione vede coinvolte in modo stretto gli utenti del sistema. Ciò richiede un piano di formazione rivolto ad ogni dipendente che utilizza le risorse informatiche dell'organizzazione. L'obbiettivo è quello di creare la "cultura della sicurezza" attraverso una serie di attività volte ad illustrare i provvedimenti ed i comportamenti da adottare per migliorare la sicurezza nel trattamento dei dati. Il piano è stato studiato, organizzato e suddiviso sulla base delle specifiche esigenze di ciascuna area in relazione alla natura dei dati trattati e dei rischi generici o specifici che incombono sui dati, nonché dei criteri e delle modalità di evitare tali rischi.

Periodicamente il responsabile dei sistemi informativi del Comune trasmette a tutti i dipendenti del materiale informativo in cui sono riportate le principali regole di gestione ed utilizzo delle risorse del sistema informativo.

13.1 Piano di formazione

Per le risorse umane, che hanno un ruolo chiave nel trattamento di dati personali, è stato fatto un corso di formazione inerente i principi fondamentali del REU 679/2016. I contenuti essenziali del piano di formazione sono:

- ragioni della nuova normativa
- ambito di applicazione materiale e territoriale
- principi generali
- diritti dell'interessato
- titolare e responsabili del trattamento
- data Protection Officer
- obbligo di tenuta di un "Registro delle attività di trattamento" ed effettuazione della "valutazione di impatto sulla protezione dei dati"
- obblighi di consultazione con l'autorità di controllo
- codici di condotta e certificazione
- trasferimento dei dati e problematiche di diritto extracomunitario
- principi legislativi e comunitari
- funzionamento della normativa nell'ambito dei diritti del cittadino
- crimini informatici, frodi, abusi, danni, casistica
- rischi possibili e probabili cui sono sottoposti i dati
- misure di sicurezza tecniche ed organizzative e comportamentali deputate alla prevenzione dei rischi
- comportamenti e modalità di lavoro per prevenire i rischi

Tale formazione viene erogata mediante supporti informativi cartacei, elettronici e/o telematici.

Il piano di formazione verrà erogato anche per i dipendenti neo assunti che nell'ambito delle loro mansioni svolgono un ruolo di responsabili del trattamento dei dati.

14 GESTIONE DEI FORNITORI A CUI SONO ASSEGNATI DEI SERVIZI CHE PREVEDONO IL TRATTAMENTO DI BANCHE DATI

Il comune di Bellusco nell'ambito della del proprio operato ha identificato dei soggetti esterni ai quali ha affidato la gestione di alcuni servizi che prevedono il trattamento di banche dati. Questo implica che queste organizzazione trattano, assumendo decisioni autonome, queste informazioni di cui il comune è Titolare.
Per ottemperare a quanto previsto dal regolamento europeo in materi di data protection l'ente ha definito una procedura di valutazione e gestione del fornitore PO-PSI-03 nella quale sono definiti i criteri per valutare la capacità dello stesso di gestire in modo corretto queste informazioni:
La procedura prevede alcune fasi che partono dalla definizione di criteri di qualifica, prevedono un processo autorizzativo da parte del titolare a trattare determinate informazioni, e la definizione congiunta con l'ente delle policy per il trattamento dei dati secondo un iter di seguito riassunto:

- Acquisizione di informazioni inerenti le politiche del fornitore in merito alla gestione dei dati
- Definizione di criteri di Selezione del fornitore
- Qualifica del fornitore ed Inserimento dello stesso nell'elenco dei fornitori accreditati
- Autorizzazione del fornitore al trattamento dei dati quale responsabile esterno
- Criteri di sorveglianza dell'operato del fornitore se la gestione dei dati costituisce un processo critico

Rif Procedura Operativa PO-PSI-03

14.1 Qualifica dei Fornitori che trattano dati per conto del Comune

Nel caso in cui l'ente assegni all'esterno dei servizi di competenza del comune che prevedono il trattamento di dati personali, prima di procedere all'assegnazione dell'incarico devono essere verificare le misure organizzative e tecnologiche attivate in tema di trattamento dei dati.
A tale scopo il responsabile del procedimento invia al fornitore una scheda per la raccolta dei dati sia di carattere generale che inerenti le modalità di gestione delle informazioni.
La scheda presente come allegato alla procedura PO-PSI-03 deve essere restituita al responsabile del procedimento con le informazioni richieste e sottoscritta da parte del rappresentante legale del fornitore.

14.2 Valutazione delle caratteristiche del fornitore

Il responsabile del procedimento unitamente al Responsabile del sistema informativo e al DPO valuta, in funzione della tipologia del servizio che il fornitore deve erogare, se le policy di gestione dei dati sono adeguate al livello di criticità e rischio implicito nel trattamento.
Nel caso siano state riscontrate delle difformità rispetto alle politiche di sicurezza dell'ente viene fatta una comunicazione in cui si chiedono maggiori delucidazioni od un adeguamento agli standard di sicurezza previsti dal comune e presenti nelle linee guida emanate da AGID.

15 AUDIT DELLA SICUREZZA

15.1 Verifiche generali

Le verifiche sulla corretta applicazione delle misure di sicurezza per la protezione dei dati e delle informazioni gestite dal comune nel suo complesso e delle misure particolari in riferimento esplicito a quelle previste dalla legge sul trattamento dei dati personali, sono affidate ai Responsabili del trattamento al DPO e al Responsabile dei sistemi informativi che si avvale di apposite liste di controllo. Le singole funzioni sono comunque tenute alle verifiche previste nella tabella di sintesi sotto riportata.

MISURE DA VERIFICARE	OGGETTO DELLE VERIFICHE	CADENZA	RESPONSABILE
Organizzazione			
Aggiornamento GDPR/PSSI	Controlli periodici, ed aggiornamento del PSSI	periodica	DPO
Outsourcing	Verifica criteri di sicurezza dei fornitori	a Campione	Responsabile Trattamento/ DPO
Incarichi inerenti la sicurezza ed il trattamento dei dati	Controlli periodici degli incarichi, dei compiti e delle responsabilità.	periodica	Responsabile Trattamento
Analisi dei rischi	Analisi dei rischi e delle contromisure da adottare per contrastarli.	periodica	Responsabile Trattamento/ DPO
Autorizzazioni all'accesso	Almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione	periodica	Amministratore di sistema
Autorizzazioni all'accesso	Rilasciate e revocate periodicamente	costantemente	Amministratore di Sistema
Piano di formazione	Attivazione del piano di formazione per nuovi collaboratori del comune	periodica	Responsabile Trattamento/ DPO
Protezione fisica			
Protezione delle aree e dei locali	Controlli periodici degli impianti e dei sistemi di sicurezza	periodica	Responsabile servizio manutenzione
Antincendio	Manutenzione periodica secondo le indicazioni dell'installatore	periodica	Responsabile servizio manutenzione
UPS	Manutenzione preventiva UPS Secondo le istruzioni del costruttore.	periodica	Amministratore di Sistema
Controllo accessi fisici ai locali	Controlli periodici dei sistemi che regolano l'accesso agli edifici, agli archivi o alle aree ad accesso ristretto.	periodica	Responsabile servizio manutenzione
Protezione Logica			

Criteri e procedure per assicurare l'integrità dei dati	Controlli accessi banche dati. Controllo utilizzo modalità di autenticazione	periodica	Amministratore di Sistema
Codici identificativi personali	Disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore	Sempre	Amministratore di Sistema
Restrizioni di accesso per via telematica	Controllo account sistema informativo	periodica	Amministratore di Sistema
Sicurezza delle trasmissioni dei dati	Controlli periodici log dei firewall	mensile	Amministratore di Sistema
Sistema Informativo			
Misure di sicurezza della rete informatica	Verifica buon funzionamento Verifica aggiornamento	periodica	Amministratore di Sistema
Patching	Aggiornamento periodico dei sistemi informativi dei server Aggiornamento periodico dei sistemi informativi dei client	Ogni mesi	Amministratore di Sistema
Back-up Dati	Verifica back-up dei dati e dei dati di sistema e efficienza apparecchiature e supporti.	Quotidiana	Amministratore di Sistema
Re impiego dei supporti di memorizzazione	Controlli sulla recuperabilità delle informazioni precedentemente contenute	costantemente	Amministratore di Sistema

16 Elenco delle Procedure allegate al presente documento

Id Procedura	Descrizione	Responsabile archiviazione
PO-PSI-01	Gestione utenti del sistema informativo	Ufficio Innovazione e Comunicazione
PO-PSI-02	Gestione delle copie di sicurezza dei dati	Ufficio Innovazione e Comunicazione
PO-PSI-03	Gestione dei fornitori a cui sono stati affidati dei trattamenti	Ufficio Innovazione e Comunicazione
PO-PSI-04	Gestione dell'informativa e del consenso al trattamento dei dati	Ufficio Innovazione e Comunicazione

PROCEDURA PER L'USO DELLE RISORSE DEL SISTEMA INFORMATIVO

Comune di Bellusco

(Provincia MB)

01	25 Mag. 2018	Prima Emissione	Amministratore di Sistema	Titolare Trattamento dei Dati
Rev.	Data	Causale	Preparato da	Approvato da

Sommario

1 Premessa

La legislazione Europea prevede sanzioni per le organizzazioni che non definiscano e adottino regole di gestione del sistema informativo e policy di sicurezza e riservatezza per il trattamento dei dati personali. L'entrata in vigore del Regolamento (UE) 679-2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, introduce rilevanti obblighi a carico degli enti pubblici, sanzionati civilmente, imponendo di gestire i dati personali rispettando il diritto di libertà e riservatezza degli interessati, prescrivendo all'organizzazione un trattamento lecito e corretto nel rispetto delle finalità per la quale i dati sono stati acquisiti.
Il presente Regolamento si pone l'obiettivo di creare una "buona pratica" nella gestione delle risorse del sistema informativo improntata alla trasparenza e all'uniformità dei comportamenti. Esso intende, pertanto, garantire Il Comune di Bellusco, che attraverso il regolamento intende definire delle regole di comportamento da parte degli utenti del sistema di gestione delle informazioni; ma anche i lavoratori che vengono, in tal modo, resi edotti della politica adottata in materia di utilizzo di risorse informatiche e di trattamento dei dati.

2 Gestione del Regolamento

2.1 Distribuzione ai soggetti interessati

Il regolamento adottato dal Comune di Bellusco, ha lo scopo di disciplinare l'utilizzo delle risorse del sistema informativo comunale.

Il regolamento si rivolge:

- ai dipendenti dell'ente;
- al personale non dipendente legato da un contratto di lavoro subordinato, di prestazione d'opera occasionale, da rapporti di collaborazione occasionali;

La presente Policy si rivolge anche a coloro che prestano il proprio lavoro regolato da un contratto di servizio o di appalto presso la sede del Comune o in un luogo diverso collegandosi al sistema informativo dell'ente per il mezzo della tecnologia informatica.

Il presente manuale viene consegnato ai soggetti precedentemente identificati da parte dell'ufficio del personale dell'ente.
Eventuali variazioni del presente regolamento vengono rese disponibili nella intranet dell'Ente.

2.2 Revisione del Regolamento

L'emissione e la revisione del Regolamento di utilizzo delle Risorse del Sistema Informativo, è gestita dal Titolare che garantisce l'aggiornamento dello stesso in modo congruente con l'evoluzione dell'organizzazione dell'ente e delle tecnologie informatiche adottate.

3 Ruoli

I ruoli previsti nella gestione del sistema informativo comunale e dal R-UE 679/2016 sono i seguenti:

Titolare: a cui competono le decisioni in ordine alle finalità, ai principi e alle modalità del trattamento dei dati;

Il **Responsabile del Sistema informativo** è incaricato Unitamente al DPO (data Protection Officer) ad:

- elaborare e stabilire le regole per un utilizzo ragionevolmente sicuro del sistema informativo comunale, in attuazione delle direttive del titolare;
- rendere operative, mediante il personale del settore elaborazione dati e/o di personale incaricato interno/esterno, le regole di sicurezza sul sistema informativo comunale;
- controllare i sistemi, con l'ausilio del personale del settore elaborazione dati e/o di personale incaricato, per individuare un eventuale uso scorretto, nel rispetto della privacy degli utenti;
- segnalare prontamente al Dirigente di riferimento, o al Titolare ogni eventuale attività non autorizzata sul sistema informativo comunale.

I **Responsabili del Trattamento** dei dati sono tenuti a:

- informare i dipendenti sull'uso appropriato delle dotazioni informatiche messe a disposizione;
- informare il personale dipendente e/o assimilato sulle disposizioni in merito all'uso consentito delle risorse del sistema informativo comunale;
- verificare che il personale loro assegnato si uniformi alle regole ed alle procedure descritte nel presente regolamento;
- verificare che i fornitori e/o il personale incaricato esterno si uniformino alle regole ed alle procedure descritte nel presente regolamento;
- adempiere a tutti gli obblighi inerenti la responsabilità in materia di trattamento di dati personali e sensibili;
- accertarsi della corretta registrazione degli accessi effettuati dagli utenti del servizio pubblico di consultazione Internet, nei settori dove è erogato tale servizio;
- segnalare prontamente all'amministratore di sistema ogni eventuale attività non autorizzata sul sistema informativo comunale.

L'amministratore del Sistema Informativo

Ha il compito di

- attuare le regole e le policy di sicurezza informatica del comune.
- sovraintendere al corretto funzionamento della rete informatica adottando policy e soluzioni tecnologiche condivise con il Responsabile dei Sistemi informativi.
- configurare e gestire gli apparati del sistema informativo comunale
- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;
- segnalare o proporre miglioramenti nell'ambito del sistema informativo al proprio responsabile.

Gli **Utilizzatori del Sistema Informativo** sono responsabili per ciò che concerne:

- il rispetto delle regole per l'uso delle risorse del sistema informativo Comunale;
- ogni uso che venga fatto delle credenziali di autenticazione assegnate secondo le modalità indicate nel presente regolamento;
- la pronta segnalazione al competente Responsabile/Titolare di ogni eventuale attività non autorizzata sul sistema informativo di cui vengano a conoscenza.

4 Regole generali

Gli utenti devono utilizzare le risorse del sistema informativo prestando attenzione a non compromettere il funzionamento e l'efficienza della rete informatica.
Devono inoltre prestare attenzione alle modalità con cui vengono utilizzate le banche dati di cui l'ente è titolare al fine di gestire in modo corretto, secondo principi di liceità e nel rispetto delle normative e regolamenti in tema di trattamento dei dati.
Gli strumenti assegnati dal Comune ai dipendenti, nonché le risorse ed i servizi del sistema informativo (accesso ad internet e posta elettronica) devono essere utilizzati unicamente per scopi ***inerenti l'attività lavorativa***.
Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento è perseguibile con provvedimenti disciplinari nonché con le azioni civili.

5 Accesso alle risorse del Sistema informativo

Le autorizzazioni di accesso al sistema informativo sono assegnate in funzione del ruolo di ogni utente in relazione all'incarico e alle relative autorizzazioni al trattamento dei dati.
Le richieste di autorizzazione all'accesso al sistema informativo comunale devono essere trasmesse dal Responsabile del Trattamento dei Dati al Responsabile dei Sistemi Informativi. Il personale autorizzato ad accedere al sistema informativo è soggetto al presente regolamento.
Il personale esterno incaricato dall'Ente (es. consulenti, stagisti, personale interinale) può accedere ai servizi del sistema informativo nei locali dell'ente previa accettazione del presente regolamento.
Le richieste di autorizzazione all'accesso devono essere trasmesse dal competente dirigente all'amministratore di sistema.
Tutti gli utenti devono prendere visione ed accettare i termini del presente regolamento tramite la sottoscrizione del "Modulo di presa visione ed accettazione del Regolamento".

5.1 Regole di autenticazione al sistema informativo Comunale

Ciascun dipendente/utente è identificato con un username personale di identificazione a cui è associata una password per l'accesso.
La username e la password personale sono gli strumenti fondamentali per garantire la sicurezza di accesso alle banche dati e alle risorse del sistema informativo dell'ente, nonché dell'indirizzo di posta elettronica comunale assegnato al singolo dipendente.
Sulla base delle regole di gestione dei codici di autenticazione, ogni utente è tenuto a determinare:

- la propria password personale di accesso alla rete comunale,
- i codici di accesso agli applicativi software dell'ente,
- la password di accesso alla casella di posta elettronica

L'accesso e l'uso sia del personal computer dell'ente, che di ogni altro sistema informatico (applicativi software, posta elettronica inclusa) è consentito solo previa identificazione dell'utente stesso tramite username e successiva digitalizzazione della password personale di accesso alle risorse e ai servizi del sistema informatico.
Il comune adotta vari livelli di autenticazione:

Password di rete
La Password è composta da almeno otto (8) caratteri alfanumerici, non deve contenere riferimenti agevolmente riconducibili alla persona (ad es. nomi dei familiari, date di nascita, ecc.) e va modificata al primo utilizzo e, successivamente, almeno ogni sei (3) mesi;

Password degli applicativi usati nei vari uffici
Valgono le stesse regole per la password di rete

Password di accesso alla posta elettronica
Valgono le stesse regole per la password di rete

Password di accesso alle banche dati esterne:
Valgono le stesse regole per la password di rete

La Password è un dato personale e non deve essere comunicata a terzi;
Rivelare la propria password o altre credenziali individuali a terzi costituisce violazione sia dei diritti fondamentali degli interessati, ai quali si riferiscono i dati contenuti negli archivi, sia delle norme interne che impongono principi di corretta gestione delle informazioni, oltre ad esporre a rischio anche la riservatezza dei dati personali riferibili all'utente;
Si deve evitare di memorizzare le password di posta elettronica o di accesso a siti web attraverso le funzionalità messe a disposizione dalle applicazioni.
Qualora si sospetti che la propria password non sia più segreta e riservata è necessario contattare immediatamente l'Amministratore del Sistema e procedere a cambiare la password.
A parziale deroga di quanto previsto al punto precedente, per consentire il regolare svolgimento delle attività di lavoro, in caso di assenze pianificate (ferie, permessi e trasferte) di qualunque durata esse siano, ogni dipendente/utente autorizza il responsabile dell'Area designato per l'accesso agli strumenti informatici e banche dati comunali, durante il periodo di assenza.

5.2 Accesso alle Banche Dati digitali

Ogni collaboratore è autorizzato ad accedere alle banche dati del sistema informativo comunale rilevanti per la sua funzione e le relative mansioni. L'autorizzazione all'accesso è perciò limitata in via esclusiva all'ambito, alla categoria di dati, alle modalità e al tempo stabilito dal relativo rapporto contrattuale e/o in eventuali comunicazioni successive;
L'accesso banche dati del sistema informatico riservate ad altri Incaricati è vietata e le richieste di accesso dovranno essere preventivamente inviate, per iscritto, al Titolare, il quale è l'unico a poter autorizzare l'Amministratore delle password a consentire l'accesso ad altre aree;
E' vietato lasciare incustodito ed accessibile il computer durante una sessione di trattamento dei dati;
I dati devono essere conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti e successivamente trattati. I tempi di conservazione dei documenti sono descritti nel manuale di gestione del protocollo.
Alla luce di ciò, in caso di allontanamento anche temporaneo dal posto di lavoro, l'incaricato dovrà verificare che non vi è possibilità da parte di terzi di accedere a dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato.

6 Comunicazione dei dati

La comunicazione di dati personali con altri enti pubblici è consentita nel caso in cui questa sia definita ed autorizzata da normative nazionali o regionali o da regolamenti.
La trasmissione di dati a soggetti privati è autorizzata nel caso di un accordo di collaborazione in cui è previsto lo scambio di informazioni. In questo caso devono essere adottate delle procedure per verificare le regole di trattamento e le misure di sicurezza adottate dal fornitore.
I dati personali trattati potranno essere comunicati all'esterno delle sedi del Titolare solo con l'autorizzazione scritta dello stesso o del Responsabile, se designato.
La trasmissione di dati personali in Paesi non appartenenti all'Unione Europea, sono autorizzati solo se sussistono le condizioni previste dal Regolamento Europeo 679/2016 sul trattamento dei dati e successive aggiornamenti normativi o regolamenti che disciplinano la materia.
Nel caso di comunicazioni/trasmissioni all'estero di dati personali deve essere data evidenza attraverso l'informativa inerente il trattamento dei dati.

7 Utilizzo delle Risorse del Sistema Informativo

Ogni incaricato è responsabile del corretto utilizzo e della custodia dei mezzi informatici consegnati.
Le banche dati, le risorse e gli strumenti del sistema informativo devono essere utilizzate unicamente per scopi attinenti all'attività lavorativa.
Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Al termine del rapporto di lavoro le attrezzature informatiche devono essere riconsegnate in buono stato con memorizzati i dati raccolti, prodotti ed elaborati durante l'attività lavorativa.

7.1 Utilizzo del Computer

Il Personal Computer affidato al dipendente è uno strumento di lavoro che deve essere usato in modo corretto. L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Amministratore del Sistema.
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita dell'Amministratore del Sistema, perché sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli installati sul computer nel momento in cui lo stesso viene consegnato all'utente (D.lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore).
Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Amministratore del Sistema.
Lasciare un elaboratore 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.
Si devono mettere in atto accorgimenti tali per cui il computer non resti incustodito, durante una sessione di trattamento: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta e accessibile; può essere sufficiente attivare lo screen saver con password oppure chiudere a chiave la stanza dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.
Non è consentita l'installazione sul proprio PC di alcun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, router, ecc.), se non con l'autorizzazione espressa del Responsabile dei Sistema Informativo.
Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
Non è consentita la memorizzazione di documenti informatici di natura personale (fotografie, file di varia natura) sugli strumenti di elaborazione o di memorizzazione comunale.

7.2 Utilizzo di Computer Portatili

L'assegnatario di un computer portatile deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.
Nel caso di spostamenti al di fuori della sede di lavoro non deve essere lasciato nel mezzo di trasporto o in luoghi non presidiati.
I PC portatili utilizzati all'esterno (convegni, seminari ecc), in caso di allontanamento, devono essere custoditi in un luogo protetto.
Se si ha in dotazione un PC portatile, si devono seguire le procedure di aggiornamento del software di protezione da virus, non si devono custodire dati di particolare rilevanza sul computer; nel caso di furto verrebbe inevitabilmente compromessa la riservatezza degli stessi.

7.3 Utilizzo dei Supporti Removibili (CD, dischi/dispositivi USB)

Prima di collegare un supporto di memoria esterno ad un PC o a un server è necessario fare controllare il supporto al software antivirus, questo in modo particolare anche nel caso di copia di file memorizzati sul supporto removibile.
Tutti i supporti riutilizzabili (pendrive, CD/DVD, dischi usb) contenenti dati comunali e dati personali devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Una persona esperta potrebbe infatti recuperare i dati memorizzati anche dopo la loro cancellazione logica.
I supporti magnetici contenenti dati personali devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti.
Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono essere abbandonati, ma si devono porre in essere gli opportuni accorgimenti finalizzati a rendere non leggibili e non ricostruibili tecnicamente i dati in essi contenuti, al fine di impedire che essi vengano carpiti da persone non autorizzate al trattamento. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.
I supporti informatici contenenti dati personali devono essere custoditi in archivi chiusi a chiave.
Non è consentito scaricare file contenuti in supporti rimovibili non aventi alcuna attinenza con la propria prestazione lavorativa.
Tutti i file di provenienza incerta od esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo da parte di software antivirus.
Ogni incaricato deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Amministratore di Sistema nel caso in cui siano rilevati virus ed adottando quanto previsto dal presente Regolamento relativo alle procedure di protezione antivirus.
Nel caso di utilizzo P.C. portatili accessibili per mezzo di smart card o tessere magnetiche in possesso a proprio uso esclusivo, ogni incaricato dovrà conservare (es. non abbandonandole sulla scrivania) e proteggere (es. non avvicinarle a fonti di calore) tali dispositivi con la massima cura. Per tutelarsi in caso di furto, è altresì necessario, per l'accensione del relativo strumento elettronico, associare a tali dispositivi una password.

7.4 Configurazione della postazione di lavoro e degli apparati di rete

La configurazione base dell'hardware e l'installazione del software nelle postazioni di lavoro e negli apparati di rete è stabilita e predisposta dal personale del settore informatico o da personale esterno incaricato.
L'utente è tenuto a non modificare la configurazione base della postazione di lavoro assegnata e degli apparati di rete messi a disposizione.
Alcuni software di utilità, individuati e resi disponibili dal settore elaborazione dati attraverso la rete comunale, potranno essere installati autonomamente dall'utente. L'installazione dei rimanenti software, dotati o meno di licenza d'uso a titolo oneroso, potrà essere effettuata solo dal personale del settore elaborazione dati o da personale interno/esterno incaricato allo scopo.

7.5 Utilizzo di hardware di proprietà personale

Non è consentito l'utilizzo di l'hardware di proprietà personale per attività lavorative che prevedano la connessione alla rete del Comune.

7.6 Policy antivirus

Malware è un nome generico che indica qualunque forma di programmi informatici maligni e indesiderati che si nascondono sotto forma di altri file.
Il *malware* minaccia in modo concreto e continuativo la sicurezza informatica e la sua eventuale diffusione nei sistemi informatici comunali può avere conseguenze molto onerose in termini di perdita di dati, mancata produttività dei dipendenti, danni all'immagine e/o alla reputazione.
Per questo, la Funzione IT ha implementato diversi controlli di sicurezza informatica che includono il rilevamento di virus, filtri contro lo spam. Benché tali forme di protezione agiscano in modalità automatica, è comunque importante conoscere i malware e saperne riconoscere gli effetti, in modo da poter contribuire alla protezione contro di essi.
I *malware* possono presentarsi in diverse forme:

- *Virus*. Può essere un programma informatico creato appositamente per replicarsi copiandosi in altri programmi presenti nel computer. Gli allegati a messaggi e-mail con estensioni come *.BAT, *.COM, *.EXE, *.SCR e *.SHS, sono un sistema comunemente utilizzato per infettare i computer attraverso l'apertura del file allegato da parte dell'utente. I virus possono alterare e danneggiare i dati, provocare il malfunzionamento dei sistemi o renderli del tutto inutilizzabili
- *Trojan horse*. Sono dei falsi programmi — file che possono risultare interessanti all'utente ma contengono codici maligni in grado di generare conseguenze come la perdita, o addirittura il furto di dati. Perché possano diffondersi occorre che essi vengano copiati sul proprio computer, ad es. aprendo un allegato di posta o scaricando un file da Internet. Essi sono usati per l'invio di e-mail di spam per indurre le persone a fornire informazioni personali, fare in modo che dati proibiti (es. immagini illegali) vengano inconsapevolmente archiviati sui computer, per lanciare attacchi a siti web per renderli indisponibili
- *Worm*. Sono programmi che si replicano automaticamente da un computer ad un altro senza alcun trasferimento di file. Tale caratteristica li distingue dai virus, che invece si diffondono attraverso file infetti (solitamente documenti di Word o Excel)
- *Spyware*. È un programma informatico che raccoglie segretamente informazioni dal computer sul quale risiede per inoltrarle ad altri senza il proprio permesso o consentire ad altri di accedere al computer infetto; gli *Adware* provocano reindirizzamenti non voluti a siti Internet specifici causando la comparsa di "pop-up" promozionali non desiderati sullo schermo del proprio computer. Spesso vengono installati sul computer poiché l'utente ha acconsentito ad installarli visitando un sito web o accettando i termini d'uso nascosti all'interno di un lungo accordo per un altro programma.

- *Bot* sono usati come strumenti di attacco remoto per prendere il controllo del computer e creare una rete di computer infetti (*Botnet*)

Il Comune di Bellusco è impegnato per garantire che i propri sistemi informativi siano privi di *malware*.

Tuttavia è necessario che tutti i dipendenti s'impegnino ad applicare alcune semplici regole, esplicitate nei seguenti paragrafi, per evitare che i *malware* possano attaccare la rete informatica del Comune e reagire adeguatamente nel caso in cui si sospetti l'infezione del proprio computer.

7.6.1 Regole per prevenire la diffusione di malware

Il Comune di Bellusco assicura che tutti gli Strumenti Informatici utilizzino il software antivirus più aggiornato; in ogni caso ciascun Utente deve prevenire la diffusione di malware adottando le seguenti regole di base:

- non disattivare mai il software per la scansione dei virus
- verificare attentamente quali dati vengono salvati sul proprio computer e la loro provenienza
- non aprire file non richiesti (es. mail o messaggi istantanei da fonti sconosciute o sospette), anche se provenienti da colleghi, chiedendo eventualmente conferma al mittente dell'invio dei file non richiesti
- non copiare, scaricare o installare file da fonti sconosciute, sospette o inaffidabili o da supporti rimovibili o freeware o shareware da Internet senza il permesso della funzione IT
- disabilitare le macro e non aprire mai allegati aventi estensioni non riconducibili a quelle normalmente utilizzate per il proprio lavoro (ad esempio, .doc, .pdf, .txt, .xls,. ppt,)
- verificare i messaggi che compaiono più di una volta nella posta in arrivo o contenenti collegamenti a siti web sconosciuti.

7.6.2 La comunicazione di possibili infezioni da malware

Nel caso in cui il software antivirus abbia rilevato la presenza di un virus o altro *malware* sul proprio computer, si ravvisi un malfunzionamento (ad es. improvvisa lentezza nell'eseguire le operazioni) è necessario contattare immediatamente l'ufficio CED attenendosi alle istruzioni che verranno impartite.

7.7 Utilizzo dei mezzi di trasmissione e riproduzione dei documenti

Nell'utilizzo di fax, stampanti, fotocopiatrici/scanner è importante adottare cautele nella trasmissione e riproduzione dei documenti contenenti dati personali e/o informazioni riservate, al fine di prevenire eventuali rischi di accesso ai dati da parte di soggetti non autorizzati sia interni che esterni.

Per quanto concerne l'utilizzo delle stampanti, l'ente mette a disposizione stampanti di rete che possono essere utilizzate contemporaneamente da più persone. A tal fine ciascun utente deve:

- non lasciare incustoditi presso il fax, la stampante di rete, la fotocopiatrice o lo scanner documenti contenenti dati personali;
- accertarsi, in caso di uso della fotocopiatrice, che non rimangano originali o copie nella macchina. In caso di cattiva qualità della stampa distruggere il supporto cartaceo e non riutilizzarlo come carta da riciclo;
- nel caso di trasmissione via fax di documenti contenenti dati personali, accertarsi telefonicamente dell'avvenuta ricezione. Una volta inviati i documenti, ritirarli immediatamente dalla macchina.

7.8 Utilizzo degli strumenti di telefonia fissa e mobile

Nell'uso di apparecchi telefonici, fissi o mobili, è possibile, anche involontariamente, rivelare informazioni che possono contenere riferimenti a dati personali e/o informazioni riservate riferite a utenti o dipendenti.

Si sottolinea quindi la necessità di applicare le seguenti accortezze:

- l'uso del telefono fisso deve avvenire utilizzando un tono di voce tale da non mettere in condizione colleghi o altre persone che possono trovarsi nelle vicinanze di comprendere l'oggetto della telefonata;
- nel corso di conference call le porte delle sale o degli uffici utilizzati devono essere chiuse.
- l'uso del telefono cellulare in spazi esterni o interni del comune per telefonate di lavoro va effettuato tenendo conto del fatto che altre persone possano sentire la comunicazione.
- L'uso dei dispositivi di telefonia mobile per fini privati deve essere fortemente limitato a casi di effettiva e comprovata necessità.

7.9 Clear desk policy

L'uso di spazi comuni adibiti a riunioni e/o postazioni di lavoro richiede che ciascun dipendente:

- presti particolare attenzione a fogli, schemi, appunti o qualsiasi altro documento dal quale sia possibile dedurre anche indirettamente informazioni a carattere personale o comunque riservato riferibili a individui;
- al termine della riunione l'eventuale materiale cartaceo prodotto deve essere rimosso o distrutto.

Tale livello di attenzione va esteso anche alle attrezzature presenti nella sala (ad es. lavagne o altri supporti cartacei) evitando accuratamente di lasciare informazioni che possano ricondurre a soggetti individuati.

Nel caso di utilizzo di sistemi di videoconferenza è opportuno che vengano rispettate le seguenti cautele:

- l'accesso agli spazi adibiti a videoconferenza deve essere autorizzato
- ogni eventuale registrazione video deve essere effettuata in modo da evitare che informazioni riservate siano distribuite, diffuse o comunicate a soggetti estranei o non autorizzati.

7.10 Uso della posta elettronica

La casella di posta, **assegnata all'utente**, è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
Si rammenta che i sistemi di posta elettronica non consentono al momento di garantire la riservatezza delle informazioni trasmesse, si raccomanda agli utenti un utilizzo accorto del servizio.
È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list non attinenti alla propria attività o funzione svolta per il Comune, salvo diversa ed esplicita autorizzazione.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per il Comune, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Titolare o dai Responsabili.
Per la trasmissione di file all'interno dell'ente è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati, se di dimensioni consistenti si consiglia di utilizzare le directory di scambio presenti sui file server, notificando a mezzo mail al destinatario la disponibilità del file stesso.
È consigliabile controllare con il software antivirus i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).
I dettagli delle regole di backup e di conservazione degli archivi di posta elettronica sono esplicitati nel piano di sicurezza o nella procedura di backup comunale.
È vietato inviare catene telematiche (o di "Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente all'Amministratore del Sistema. Non si deve in alcun caso attivare gli allegati di tali messaggi.
Nel caso di assenza di un dipendente il responsabile di Area potrà avere accesso alla casella di posta elettronica del dipendente per motivi legati alla gestione delle attività lavorative dell'ufficio, dandone comunicazione al dipendente.
Con riferimento ai trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro, come già precisato dal Garante in precedenti occasioni, in conformità ai principi in materia di protezione dei dati personali, gli account riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento (indirizzo dell'Ufficio).
I contenuti delle caselle di posta personale dei dipendenti che si dimettono vengono conservate per 6 mesi al termine del quali i contenuti della casella verranno cancellati.

7.11 Uso della rete Internet e dei relativi servizi

L'ente ha installato apparati per il monitoraggio degli accessi alla rete di internet unicamente per scopi di sicurezza.
Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È proibita la navigazione in Internet per motivi diversi da quelli funzionali all'attività lavorativa stessa.
È vietato all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal Responsabile dei Sistemi Informativi.
È vietata effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dai dirigenti o attinenti i compiti e le mansioni assegnate e con il rispetto delle normali procedure di acquisto.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
È vietata la partecipazione a forum non professionali, l'utilizzo di chat (esclusi gli strumenti autorizzati), di bacheche elettroniche anche utilizzando pseudonimi, se non attinenti l'attività lavorativa svolta.
Il Servizio Sistemi Informativi si riserva di applicare per singoli e gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con il titolare e con i Responsabili, al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
Non è consentita la navigazione in siti ove sia possibile rivelare le opinioni politiche, religiose o sindacali dell'utilizzatore; non è consentito inoltre visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso/etnia/religione/opinione e/o appartenenza sindacale e/o politica.
Nella prospettiva della prevenzione di cui al presente documento l'ente si riserva la facoltà di adottare software o apparati hardware volti a bloccare l'accesso a determinati siti a contenuto estraneo all'attività dell'ente. Questo tipo di sistemi con modalità automatiche di filtro e inibizione non comporta un controllo diretto o indiretto sulla posizione individuale, ma semplicemente può impedire l'accesso a determinati siti non funzionali all'attività istituzionale dell'ente, può impedire il downloading di materiale, funge da filtro per il virus detecting, impedisce l'invio o la ricezione di mail contenenti determinate parole (a sfondo sessuale o razzista) o di determinate dimensioni.
Il Comune ha attivato dei sistemi di monitoraggio del traffico web che salvano gli indirizzi delle pagine a cui un determinato computer ha avuto accesso. I file con i dati di navigazione vengono conservati per sei mesi e poi cancellati. L'amministratore di sistema ha la facoltà di accedere e controllare i dati della navigazione in modo anonimo per motivi di sicurezza della rete informatica e delle banche dati gestite dell'ente.

7.12 Gestione delle banche dati e dei file di ufficio

Ad ogni dipendente dotato di una postazione di lavoro fornita dall'ente è normalmente riservato uno spazio sul disco locale ed eventualmente una cartella su server ed una o più cartelle condivise sui dischi accessibili attraverso la rete telematica comunale. L'utilizzo di tali risorse è strettamente riservato all'archiviazione ed alla condivisione dei file necessari alla normale attività lavorativa.
Per lo scambio e la condivisione temporanea di file viene messa a disposizione un'area dei dischi di rete.
L'utente è tenuto alla periodica (almeno ogni sei mesi) pulizia di tutti gli spazi assegnati, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati al fine di evitare, salvo casi eccezionali, un'archiviazione superflua.
Il personale del settore informatico dati ha la facoltà di rimuovere i file degli utenti, senza preavviso, in caso di necessità di spazio sui dischi di rete, spostandoli su altri dispositivi di memorizzazione, o di rinominare i nomi delle cartelle o dei file in caso di malfunzionamenti.
I dati contenuti nelle cartelle condivise dei dischi di rete, ad eccezione dell'area di scambio, vengono salvati periodicamente con delle procedure di backup a cura del personale del settore elaborazione dati. È fatto obbligo per gli utenti del sistema informativo comunale salvare i dati importanti su server di rete.
I dettagli delle regole di backup e di conservazione dei dati sono esplicitati nel piano di sicurezza o nella procedura di backup comunale.
Le richieste di recupero dei dati vanno inoltrate, non appena se ne manifesti la necessità, al personale del settore informatico, che si riserva di verificare la possibilità di recupero dei dati compatibilmente con le esigenze di servizio

7.13 Sito Internet

I dipendenti comunali autorizzati possono pubblicare pagine informative e modulistica sul sito internet istituzionale, utilizzando gli strumenti di redazione messi a disposizione dal sistema informativo.
I responsabili di ufficio che provvedono autonomamente alla redazione delle pagine pubblicate sul sito internet, sono responsabili dei contenuti pubblicati.
Qualora la redazione dei contenuti sia affidata a società esterne o a consulenti, i responsabili di settore devono validare ad approvare i contenuti pubblicati.
Il personale del settore informatico fornisce l'assistenza necessaria a garantire il funzionamento degli ambienti di redazione e pubblicazione, ma non è tenuto a fornire assistenza sulle pagine realizzate dagli utenti.
Il responsabile del sistema informativo, avvalendosi di procedure automatiche o manuali, può provvedere all'aggiornamento degli ambienti di redazione ed alla rimozione dei contenuti dall'area pubblica, senza necessità di preavviso.
Le regole di pubblicazione di dati e informazioni nell'albo pretorio e definito da una linea guida.

8 Gestione dei documenti cartacei

Gli incaricati del trattamento devono prelevare dagli archivi/armadi i soli atti e documenti loro affidati, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio/armadi, al termine di tale ciclo.

Per gli atti ed i documenti contenenti **dati personali particolari (sensibili)** o dati giudiziari, il controllo e la custodia devono avvenire in modo tale che ai dati non accedano persone prive di autorizzazione.
In questo caso è quindi necessario che l'incaricato del trattamento utilizzi **cassetti con serratura, o altri accorgimenti** aventi funzione equivalente, nei quali riporli prima di assentarsi dal posto di lavoro, anche se temporaneamente. In tali cassetti i documenti potranno essere riposti al termine della giornata di lavoro, qualora l'incaricato debba utilizzarli anche nei giorni successivi; al termine del trattamento l'incaricato dovrà invece restituirli all'archivio.
Per gli accessi agli archivi contenenti dati sensibili che avvengono dopo l'orario di chiusura, è obbligatorio identificare e registrare coloro che vi accedono.

9 Trattamenti di dati ed informazioni relative all'uso del sistema informativo

9.1 Prevenzione

Ai fini della prevenzione degli accessi non autorizzati e degli abusi nell'utilizzo dei servizi offerti dal sistema informativo comunale, saranno prese tutte le misure tecniche ed organizzative ritenute idonee, incluso l'utilizzo di strumenti automatici quali la registrazione degli accessi, gli strumenti di verifica del software e dell'hardware in uso sulle postazioni di lavoro e la registrazione dei collegamenti alle reti Intranet/Internet.
Nel pieno rispetto della normativa vigente, il Comune si riserva il diritto di verificare l'attuazione delle disposizioni del presente regolamento anche attraverso l'analisi dei dati registrati nei file di log degli apparati del sistema informativo comunale.

9.2 Registrazioni

Il sistema informativo comunale è basato sul dominio di rete che gestisce tutte le risorse informatiche registrate in un dominio Active Directory.
I sistemi di elaborazione effettuano le seguenti registrazioni delle attività in file di log delle seguenti tipologie e con le seguenti politiche di conservazione:

- Per ogni sistema avviene la registrazione degli eventi legati alle applicazioni, alla protezione del sistema ed al sistema stesso. La conservazione ha durata limitata a 3 mesi al fine di poter analizzare eventuali problemi di sicurezza.
- I server del sottosistema di configurazione dinamica degli indirizzi di rete (DHCP – Dinamyc Host Configuration Protocol) conservano le registrazione delle allocazioni degli indirizzi di rete alle stazioni di lavoro. La conservazione ha durata limitata a 3 mesi.
- Il server di posta elettronica conserva tutte le mail degli utenti, nei limiti dello spazio disco a disposizione e delle regole di conservazione definite, e conserva le registrazioni degli elementi di descrizione del traffico di posta elettronica. Tutte le registrazioni possono essere consultate unicamente dall'amministratore di sistema e dal titolare per scopi legati alla verifica del buon funzionamento del sistema informativo comunale e per motivi di sicurezza.

9.3 Controlli sull'Uso delle Risorse del Sistema Informativo

I dati registrati potranno essere aggregati per svolgere controlli finalizzati ad evitare abusi nell'uso di Internet o per determinare le cause di eventuali malfunzionamenti del sistema.
I controlli verranno effettuati dall'amministratore di sistema e dal personale del settore informatico per verificare la sicurezza della rete comunale e prevenire o risolvere eventuali problemi di sicurezza.
In particolare, l'Amministratore di Sistema per le verifiche seguirà le seguenti procedure:

- Internet: verranno visionati, attraverso specifica reportistica ottenuta tramite programmi di analisi Log e in forma anonima, le tipologie di accesso (https, ftp, ecc.), il numero di accessi e di visualizzazione delle pagine, le ore di utilizzo totali e le fasce orarie di utilizzo, i tentativi di intrusione dalla rete internet verso la rete comunale o la singola postazione informatica del comune.
- Posta elettronica: analisi dei flussi di ricezione e spedizioni e-mail dall'indirizzo di posta elettronica comunale assegnato a ciascun utente, con esame dei dati relativi alla frequenza ed alla tipologia di anomalie nella spedizione/consegna del messaggio, oltre che nella ricezione dello stesso.
- Rete interna: verranno verificati i tentativi di intrusione ed accesso alle risorse comunali (file e cartelle) protette, sia di quelle presenti in rete che non. Inoltre, sarà verificato il numero di accessi complessivi ed ogni tentativo di accesso negato a risorse comunali protette.

Ogni abuso nell'uso del sistema informativo sarà comunicato alle figure indicate nel cap 3 Ruoli.
L'amministratore di sistema, su richiesta dell'autorità giudiziaria o delle forze di polizia, previa autorizzazione del titolare, potrà in ogni momento fornire i dati registrati dal sistema.

10 Data Breach (violazione dei dati personali)

I dati personali conservati, trasmessi o trattati dall'ente possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati.
Nel caso in cui l'utente del sistema informativo riscontri una violazione delle banche dati dell'ente contenenti dati personali ne deve dare immediata informazione al Titolare o al Responsabile del sistema informativo.
Il titolare deve avviare una procedura di comunicazione all'autorità garante del trattamento dei dati come previsti all'articolo 33 e 34 del R- UE 679/2016 .

11 Incarico per il Trattamento dei Dati

Il RUE 679/2016 disciplina la gestione dei dati personali ed impone che all'interno di ogni ente sia costituita una gerarchia, comprendente le figure del titolare, del responsabile del trattamento, funzionale alla sua applicazione. Tale gerarchia non comporta alcuna modifica della qualifica professionale o delle mansioni assegnate ai dipendenti.
Ogni singolo Impiegato è autorizzato al trattamento di dati personali (dato che nell'ambito dello svolgimento delle proprie funzioni viene necessariamente a conoscenza dei contenuti delle banche dati presenti presso la propria unità operativa) nell'ambito delle mansioni ad esso assegnate. Le banche dati cui potrà accedere per il trattamento - previa abilitazione ed indicazione delle modalità di utilizzo - sono unicamente quelle previste per il ruolo assegnato identificato nel documento di incarico al trattamento dei dati.
Per il trattamento di dati deve intendersi: "operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati"

Bellusco li

Il dipendente del Comune per presa Visione

Comune di Bellusco

Data Aggiornamento 25-5-2018

Elenco dei Server

Nome Server/Servizio/Apparato	Sistema Operativo	Software e Servizi	Software Virtualizzazione Server	configurazioni di Sicurezza / Protezione	Ubicazione
Server fisico	windows server 2012	applicative sicra - cartelle utenti - Sapignoli - Crux	No	Macrium reflect - backup windows server su disco esterno - RAID 5 + Antivirus	Stanza server piano Terra
Server	windows 2008	Planet web e xpers - File server e gestione dei backup	No	RAID 5 - anMacrium reflect - backup windows server su disco esterno - RAID 5 + Antivirustivirus	Stanza server piano Terra
Servizio di posta elettronica	Hosting	Associazione pinamonet			
Server aruba business	Backup cloud	Backup delle cartelle e data base degli applicativi		Macrium reflect - backup windows server su disco esterno	

Comune di Bellusco

Data Aggiornamento 25-05-2018

Servizio/Applicativo	Nome del software	Fornitore/Manuten.	Regole di autenticazione applicativa	Regole di gestione	Profilazione utente
Gestione Biblioteca	Cubinrete	Sistema Bibliotecario dell'Est di Milano	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione navigazione utenti biblioteca	Cubinrete	Sistema Bibliotecario dell'Est di Milano	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione Pratiche edilizie	Archi7	Starch srl	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione Presenze	Planet Time	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Elaborazione cedolini paghe	Jpers	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione programma Messi	Sicr@web	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione Ragioneria	Sicr@web	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione Protocollo	Sicr@web	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione rette servizio scuola	Sicr@web	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione Segreteria	Sicr@web	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione Tributi	Sicr@web	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione Protocollo	Sicr@web	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista
Gestione Demografico	Sicr@web	Maggioli SpA	id e password	Complessità	Funzionale Periodicamente Rivista

Gestione Cimitero	Crux	Starch srl	id e password	Complessità	Funzionale Periodicamente Rivista
Posta elettronica	Pinamonte	Brianza est	id e password	Complessità	Funzionale Periodicamente Rivista
Servizi di portale					
Segreteria	Sito web	Panservice Latina	Nessuna autenticazione sito informativo del comune		
Segreteria	Albo Pretorio	Maggioli SpA	Nessuna autenticazione sito informativo del comune		
Ufficio Scuola	iscrizione servizi scolastici portale URBI	PA digitale	accesso tramite id + password	Scadenza Password Ogni 6 mesi, Non possibilità usare stessa psw per 1 volta	
Segreteria	Servizio di segnalazione problemi sul territorio del comune con portale Ocio	Starch Srl	accesso tramite id + password	Scadenza Password Ogni 6 mesi, Non possibilità usare stessa psw per 1 volta	
Segreteria	Denuncia Tassa rifiuti	CemAmbiente	accesso tramite id + password	Scadenza Password Ogni 6 mesi, Non possibilità usare stessa psw per 1 volta	
Edilizia Privata - SUE	Cportal	Starch Srl	accesso tramite id + password o CRS	Scadenza Password Ogni 6 mesi, Non possibilità usare stessa psw per 1 volta	
Suap Commercio	impresainungiorno		SPID e CRS	Scadenza Password Ogni 6 mesi, Non possibilità usare stessa psw per 1 volta	

Titolare del Trattamento — Comune di Bellusco - P.zza Fratelli Kennedy 1 - Bellusco — Rappresentante Legale: Sindaco Roberto Invernizzi — Data Aggiornamento 25/05/2018

Responsabile del trattamento — Dott.ssa Emanuela Ronchi — email: comune.bellusco@pec.regione.lombardia.it

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso Dati	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Biblioteca	Gestione della biblioteca	Archivio contenente l'anagrafica degli utenti e la movimentazione relativa ai prestiti.	Digitale ed analogico	Lett- Scrit	P/S	Utenti	Informativa	Cubinrete	Hosting Applicativo	Descritte nel GDPR	Sistema Bibliotecario Nord Est Milano		Personale ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Biblioteca	Gestione comunicazione per eventi culturali	Indirizzo mail e cellulare degli utenti per comunicazioni ed invio newsletter	Digitale ed analogico	Lett- Scrit	P	Utenti	Consenso	Cubinrete	Hosting Applicativo	Descritte nel GDPR	Sistema Bibliotecario Nord Est Milano		Personale ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Biblioteca	Gestione della navigazione in internet	Dati degli utenti iscritti al servizio / dati della navigazione	Digitale ed analogico	Lett- Scrit	P	Utenti	Informativa	Cubinrete	Hosting Applicativo	Descritte nel GDPR	Sistema Bibliotecario Nord Est Milano		Personale ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Biblioteca	Banche dati eventi culturali	Dati dei soggetti che partecipano agli eventi	Digitale ed analogico	Lett- Scrit	P/S	Professionisti - Rappresentante legale Azienda	Informativa	Office	File server	Descritte nel GDPR			Personale ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Biblioteca	Gestione della corrispondenza in ingresso ed in uscita	Banca dati del protocollo con corrispondenza in entrata ed in uscita	D/A	Lett- Scrit	P	Cittadini / Imprese / altri enti	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Biblioteca	Anagrafica semplificata dei cittadini e delle Imprese	dati anagrafici	D	Lett	P	Cittadini/Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Biblioteca	Gestione degli impegni, liquidazione della fatture	dati contabili/dati relativi a fatture e liquidazioni	D/A	Lett- Scrit	P/E	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Biblioteca	Gestione atti amministrativi	Dati anagrafici di cittadini/ Imprese identificati nelle delibere determine ed ordinanze	D/A	Lett- Scrit	P	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Biblioteca	Comunicazioni attraverso Posta elettronica	Corrispondenza dell'ufficio	Digitale	Lett- Scrit	P/S/G	Professionisti - Rappresentante legale Azienda	Informativa	Client Posta	Hosting	Descritte nel GDPR	Associazione Pinamonte - Brianza est		Personale Ufficio / Utenze personali	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessario

Titolare del Trattamento — Comune di Bellusco - P.zza Fratelli Kennedy 1 - Bellusco — Rappresentante Legale: Sindaco Roberto Invernizzi — Data Aggiornamento 25/05/2018

Responsabile del trattamento — Dott Giorgio Vitali — email comune.bellusco@pec.regione.lombardia.it

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso Dati	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Demografico	Gestione dell'Anagrafe dei Residenti	Dati anagrafici e dati per eventuali comunicazioni	D	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Ina/SAIA Ministero Interni	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Anagrafe cittadini residenti all'estero	Dati anagrafici	D	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	ANAG/AIRE Ministero Interni	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Cartellini Carte Identità	Dati anagrafici	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Ministero dell'interno	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Carta identità elettronica	Dati anagrafici , dichiarazione donazione organi	D	Lett- Scrit	P	Cittadini residenti	Informativa	Portale del ministero Interni	Portale del ministero Interni	Descritte nel GDPR		Ministero dell'interno	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	schede di famiglia archiviate in formato cartaceo sino al 2010 e successivamente gestite in formato digitale	Dati anagrafici	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	schede Individuali archiviate in formato cartaceo sino al 2010 e successivamente gestite in formato digitale	Dati anagrafici del nucleo famigliare	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Archivio dello stato civile	Atti di stato civile (Atti di nascita, Atti di matrimonio atti di morte)	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Gestione delle Liste elettorali	Dati anagrafici aventi diritto al voto	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Prefettura - Commissione mandamentale	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Albo scruatori e presidenti di seggio	dati anagrafici	D/A	Lett- Scrit	P/G	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Corte d'Appello	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Fascicoli inibiti al voto	Dati anagrafici inibiti al voto	D/A	Lett	P/G	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Ricevuti dal Tribunale o da altri comuni / trasmissione ad altro comune nel caso di variazione della residenza	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Giudici popolari	dati anagrafici dei giudici popolari	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Tribunale	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Gestione liste di leva	dati anagrafici persone inserite nelle liste che vengono trasmesse al distretto militare	D	Lett- Scrit	P	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Distretto Militare	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Liste anagrafiche comunali	dati anagrafici	D	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Istat	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Statistica Migrazioni ed Immigrazione	Dati aggregati	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Istat - ATS	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Scheda Istat D4 morte	Dati aggregati	D/A	Lett- Scrit	P/S	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	ATS / Prefettura	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Gestione cimiteriale Contratti / Loculi	Contratti cimiteriali e dati anagrafici defunto	D/A	Lett- Scrit	P	Cittadini	Informativa	Crux	Server Applicativo	Descritte nel GDPR	starch srl		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Demografico	Testamento biologico - DAT	dati anagrafici e desideri del soggetto	A	Lett- Scrit	P/S	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Gestione della corrispondenza in ingresso ed in uscita	Banca dati del protocollo con corrispondenza in entrata ed in uscita	D/A	Lett- Scrit	P	Cittadini / Imprese / altri enti	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Anagrafica semplificata dei cittadini e delle Imprese	dati anagrafici	D	Lett	P	Cittadini/Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Gestione degli impegni, liquidazione della fatture	dati contabili/dati relativi a fatture e liquidazioni	D/A	Lett- Scrit	P/E	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Gestione atti amministrativi	Dati anagrafici di cittadini/ Imprese identificati nelle delibere determine ed ordinanze	D/A	Lett- Scrit	P	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Gestione Gare ed Appalti	Dati anagrafici delle Imprese o dei Professionisti - Istruttoria delle gara - Casellari Giudiziali	D/A	Lett- Scrit	P	Professionisti / Imprese	Informativa	Sintel / Mepa	Portale	Descritte nel Piano di sicurezza	Regione Lombardia - Consip		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Comunicazioni attraverso Posta elettronica	Corrispondenza dell'ufficio	D	Lett- Scrit	P/S/G	Professionisti - Rappresentante legale Azienda	Informativa	Client Posta	Hosting	Descritte nel GDPR	Associazione Pinamonte - Brianza est		Personale Ufficio / Utenze personali	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessario
Demografico	Anagrafe delle prestazioni Banca dati che raccoglie gli incarichi conferiti dalle pubbliche amministrazioni sia a dipendenti pubblici che a consulenti.	Dati anagrafici delle aziende e dei professionisti	D/A	Lett- Scrit	P	Dipendenti Consulenti	Informativa	PerlaPA	Hosting applicativo	Descritte nel Piano di sicurezza			Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Gestione procedimento inerenti la trasparenza amministrativa	Dati anagrafici contabili e tecnici inerenti procedimenti del comune	D/A	Lett- Scrit	P	Dipendenti - Consulenti - Professionisti - Cittadini	Informativa	sessione del sito internet del comune - Portale trasparenza	Hosting applicativo	Descritte nel Piano di sicurezza	Opencontent S.c.a.r.l		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Demografico	Pubblicazione all'albo on line	dati dell'ufficio	D	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Sito web	Hosting Applicativo	Descritte nel GDPR		Albo on Line	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Tipologia di trattamento	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno /Titolare del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso Dati	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Informatizzazione	Gestione del sistema Informativo del comune	Dati in formato digitale dell'ente	Digitale	Lett- Scrit	P/S/G	Cittadini - Rappresentante Legale Organizzazione	Attraverso strumenti di elaborazione	Informativa	Software usati dai vari uffici del comune	Server del sistema informativo del comune	Descritte nel Piano di sicurezza	Soggetti che svolgono attività di assistenza e manutenzione		Amministratori di sistema	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Titolare del Trattamento Comune di Bellusco - P.zza Fratelli Kennedy 1 - Bellusco Rappresentante Legale: Sindaco Roberto Invernizzi Data Aggiornamento 25/05/2018

Responsabile del trattamento Dott Giorgio Vitali email comune.bellusco@pec.regione.lombardia.it

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso DB	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Protocollo Mes	Protocollazione corrispondenza in uscita	Corrispondenza in uscita trasmessa attraverso e-mail - fax -posta	Digitale ed analogico	Lett- Scrit	P/S/G	Cittadini - Aziende - Enti	Informativa	sicr@Web	Server Applicativo	Descritte nel GDPR	Maggioli Spa		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Protocollazione corrispondenza in ingresso	Corrispondenza in ingresso ricevute attraverso e-mail - fax -posta	Digitale ed analogico	Lett- Scrit	P/S/G	Cittadini - Aziende - Enti	Informativa	sicr@Web	Server Applicativo	Descritte nel GDPR	Maggioli Spa		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Atti amministrativi ai sensi del codice di procedura civile	Atti depositati e notificati che vengono depositati presso sede del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	sicr@Web	Server Applicativo	Descritte nel GDPR	Maggioli Spa	Regione	Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Gestione notifiche atti tributari	Atti depositati e notificati che vengono depositati presso sede del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	sicr@Web	Server Applicativo	Descritte nel GDPR	Maggioli Spa		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Gestione avvisi di deposito dell'agenzia delle entrate presso casa comunale	Atti depositati e notificati che vengono depositati presso sede del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	sicr@Web	Server Applicativo	Descritte nel GDPR	Maggioli Spa		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Pubblicazione Albo pretorio	Dati relativi agli atti amministrativi del comune	Digitale ed analogico	Lett- Scrit	P/S	Cittadini - Aziende - Enti	Informativa	sicr@Web	Server Applicativo	Descritte nel GDPR	Maggioli Spa		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Pubblicazione Amministrazione trasparente	Dati relativi agli atti amministrativi del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	sicr@Web	Server Applicativo	Descritte nel GDPR	Maggioli Spa		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Registrazione atti di deposito	Atti depositati e notificati che vengono depositati presso sede del comune	Digitale ed analogico	Lett- Scrit	P/S/G	Cittadini - Aziende - Enti	Informativa	sicr@Web	Server Applicativo	Descritte nel GDPR	Maggioli Spa		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Anagrafica semplificata dei cittadini e delle Imprese	Dati anagrafici	Digitale ed analogico	Lett	P	Cittadini	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli Spa		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Applicabile
Protocollo Mes	Gestione delle comunicazioni attraverso posta elettronica	Corrispondenza dell'Ufficio	Digitale	Lett- Scrit	P/S	Cittadini / Aziende / Enti	Informativa	Client Posta	Hosting	Descritte nel GDPR	Associazione Pinamonte - Brianza est		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Titolare del Trattamento — Comune di Bellusco - P.zza Fratelli Kennedy 1 - Bellusco — Rappresentante Legale: Sindaco Roberto Invernizzi — Data Aggiornamento 25/05/2018

Responsabile del trattamento — Rag Giovanna Biella — email comune.bellusco@pec.regione.lombardia.it

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno /Titolare del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso Dati	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Ragioneria	Gestione del Bilancio e tenuta dei registri contabili	Dati contabili e dati personali relativi alle registrazioni contabili	Digitale ed analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Fatture elettroniche fornitori	Dati contabili e dati personali relativi alle registrazioni contabili	Digitale ed analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Sicr@web Piattaforma Interscambio	Hosting	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Impegni e pagamenti	Dati contabili e dati personali relativi alle registrazioni contabili	Digitale ed analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Accertamenti ed Incassi	Dati contabili e dati personali relativi alle registrazioni contabili	Digitale ed analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
0	Dichiarazioni fiscali inerenti l'Ente IVA e IRAP	Dati contabili e dati personali relativi alle registrazioni contabili	Digitale ed analogico	Lett- Scrit	P	Professionisti - Rappresentante legale Azienda	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Agenzia entrate	Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione rilevazione telematica degli incassi e dei pagamenti effettuati dai tesorieri di tutte le amministrazioni pubbliche	Pagamenti su tracciati SIOPE	Digitale ed analogico	Lett- Scrit	P	Dipendenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	MEF attraverso tesoriere	Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione del Documento Unico Programmazione	Pianificazione economica finanziaria	Digitale ed analogico	Lett- Scrit	P	Dipendenti Aziende Professionisti	Informativa	Office	File server	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Certificazione unica dei compensi Lavoratori Autonomi	Dati relativi alla Certificazione unica dei compensi	Digitale ed analogico	Lett- Scrit	P	Dipendenti Aziende Professionisti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Agenzia Entrate	Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Dati inerenti incarichi, contributi e sovvenzioni, pagamenti e liquidazioni	Riscossione Ruoli	Digitale ed analogico	Lett- Scrit	P	Dipendenti Aziende Professionisti	Informativa	Sicr@web	Portale Trasparenza	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione del flusso di dati rendicontazione ANAC	Elenco delle determine , cig ed importi e ragione sociale ditte e professionisti	Digitale ed analogico	Lett- Scrit	P	Dipendenti Aziende Professionisti	Informativa	Portale ANAC	Hosting	Descritte nel GDPR		ANAC	Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Controlli nei confronti dei soggetti a cui l'ente fa dei pagamenti	Banca dati antimafia	Digitale ed analogico	Lett	P	Dipendenti Aziende Professionisti	Informativa	Portale BDNA	Hosting	Descritte nel GDPR		Prefettura	Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Controlli nei confronti dei soggetti a cui l'ente fa dei pagamenti	Dati del DURC	Analogico	Lett	P	Dipendenti Aziende Professionisti	Informativa	Office	Hosting	Descritte nel GDPR		INPS	Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Dati di alla corte dei conti		Digitale ed analogico	Lett	P	Dipendenti Aziende Professionisti	Informativa	Corte dei conti servizi on line	Hosting	Descritte nel GDPR			Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione degli agenti contabili	Dati trasmessi alla Corte dei conti	Digitale ed analogico	Lett	P	Cittadini e Dipendenti Aziende	Informativa	Sireco	Hosting	Descritte nel GDPR		corte dei conti	Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Pagamenti dei ruoli dei tributi e sanzioni amministrative	Dati relativi ai versamenti e ai contribuenti	Digitale ed analogico	Lett	P	Cittadini e Dipendenti Aziende	Informativa	Sicr@web	Hosting	Descritte nel GDPR	**Riscossore**		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione conto corrente Postale	Dati dei soggetti che fanno pagamenti attraverso conto corrente	Digitale ed analogico	Lett	P	Cittadini e Dipendenti Aziende	Informativa	Portale Poste Italiane	Hosting	Descritte nel GDPR	Poste Italiane SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione della corrispondenza in ingresso ed in uscita	Banca dati del protocollo con corrispondenza in entrata ed in uscita	D/A	Lett- Scrit	P	Cittadini / Imprese / altri enti	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Anagrafica semplificata dei cittadini e delle Imprese	dati anagrafici	D	Lett	P	Cittadini/Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione atti amministrativi	Dati anagrafici di cittadini/ Imprese identificati nelle delibere determine ed ordinanze	D/A	Lett- Scrit	P	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione Gare ed Appalti	Dati anagrafici delle Imprese o dei Professionisti - Istruttoria delle gara - Casellari Giudiziali	D/A	Lett- Scrit	P	Professionisti / Imprese	Informativa	Sintel / Mepa	Portale	Descritte nel Piano di sicurezza	Regione Lombardia - Consip		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Ragioneria	Comunicazioni attraverso Posta elettronica	Corrispondenza dell'ufficio	Digitale	Lett- Scrit	P/S/G	Professionisti - Rappresentante legale Azienda	Informativa	Client Posta	Hosting	Descritte nel GDPR	Associazione Pinamonte - Brianza est		Personale Ufficio / Utenze personali	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessario
Ragioneria	Anagrafe delle prestazioni Banca dati che raccoglie gli incarichi conferiti dalle pubbliche amministrazioni sia a dipendenti pubblici che a consulenti.	Dati anagrafici delle aziende e dei professionisti	D/A	Lett- Scrit	P	Dipendenti Consulenti	Informativa	PerlaPA	Hosting applicativo	Descritte nel Piano di sicurezza			Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Ragioneria	Gestione procedimento inerenti la trasparenza amministrativa	Dati anagrafici contabili e tecnici inerenti procedimenti del comune	D/A	Lett- Scrit	P	Dipendenti - Consulenti - Professionisti - Cittadini	Informativa	sessione del sito internet del comune - Portale trasparenza	Hosting applicativo	Descritte nel Piano di sicurezza	Opencontent S.c.a.r.l		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Titolare del Trattamento Comune di Bellusco - P.zza Fratelli Kennedy 1 - Bellusco Rappresentante Legale: Sindaco Roberto Invernizzi Data Aggiornamento 25/05/2018

Responsabile del trattamento Dott Giorgio Vitali email comune.bellusco@pec.regione.lombardia.it

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso Dati	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Segreteria Generale	Gestione Atti Amministrativi	Delibere Consiglio Comunale	Digitale	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Gestione Atti Amministrativi	Delibere Giunta Comunale	Digitale	Lett- Scrit	P/S	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Gestione Atti Amministrativi	Archivio delle Determine	Digitale	Lett- Scrit	P/S	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Pubblicato Amministrazione trasparente	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Gestione Atti Amministrativi	Ordinanze sindacali o dirigenziali	Digitale ed Analogico	Lett- Scrit	P/S	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Comunicazione verso cittadini , Altri enti , Aziende	Corrispondenza degli assessori	Digitale ed Analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Richieste accesso agli atti	Dati del richiedente	Digitale ed Analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Decreti sindacali (TSO)	Atti del sindaco	Digitale ed Analogico	Lett- Scrit	P/S	Cittadini	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Verbali nucleo di valutazione	Dati relativi al personale dell'ente	Digitale ed Analogico	Lett- Scrit	P	Dipendenti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Pubblicazione compensi amministratori	Dadi dei compensi degli amministratori	Digitale ed Analogico	Lett- Scrit	P	Amministratori	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Gestione consulte	Verbali	Digitale ed Analogico	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Gestione contenzioso per sinistri assicurativi	Dati dei soggetti coinvolti	Digitale ed Analogico	Lett- Scrit	P/S	Cittadini	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Accesso agli atti da parte di consiglieri ed amministratori	Dati generici	Digitale ed Analogico	Lett- Scrit	P/S	Cittadini - Aziende - Enti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Informazioni istituzionali da pubblicare all'albo on line	Dati generici	Digitale	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Sitoweb	Hosting Applicativo	Descritte nel GDPR		Albo on Line	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Comunicazione ai consiglieri	Dati generici	Digitale	Lett- Scrit	P	Cittadini - Aziende - Enti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Comunicazioni istituzionali	Dati generici	Digitale ed Analogico	Lett- Scrit		Cittadini - Aziende - Enti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Agenda sindaco o assessori	Dati generici	Digitale ed Analogico	Lett- Scrit	P/S	Cittadini - Aziende - Enti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Segreteria Generale	Gestione solennità civili	Dati generici	Digitale ed Analogico	Lett- Scrit		Cittadini - Aziende - Enti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Decreti sindacali (TSO)	Dati relativi ai soggetti sottoposti a TSO	Digitale ed Analogico	Lett- Scrit	P/S	Cittadini	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Segreteria Generale	Gestione situazioni crisi aziendale	Dati generici	Digitale ed Analogico	Lett- Scrit	P	Dipendenti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Staff Segretario	Verbali comitato di direzione e giunta	Dati generici	Digitale ed Analogico	Lett- Scrit	P	Dati generici	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Gestione del contenzioso	Atti e documenti per la tutela legale	Digitale ed Analogico	Lett- Scrit	P	Contraenti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Repertorio scritture private	Dati relativi al contratto e ai contraenti	Digitale ed Analogico	Lett- Scrit	P	Contraenti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Atti di disposizione del patrimonio immobiliare	Dati relativi alle concessioni o locazioni, dati dei contraenti	Digitale ed Analogico	Lett- Scrit	P	Cittadini	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Gestione dei contratti rogati dal segretario comunale	Dati relativi alla gara, dati del rappresentante legale dell'azienda e dei professionisti	Digitale ed Analogico	Lett- Scrit	P/G	Contraenti	Informativa	**Office Unimod**	file server	Descritte nel GDPR		Agenzia delle Entrate	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Contratti cimiteriali	Dati dei contratto e del soggetto che lo ha sottoscritto	Digitale ed Analogico	Lett- Scrit	P	Contraenti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Gestione della corrispondenza in ingresso ed in uscita	Banca dati del protocollo con corrispondenza in entrata ed in uscita	D/A	Lett- Scrit	P	Cittadini / Imprese / altri enti	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Anagrafica semplificata dei cittadini e delle Imprese	dati anagrafici	D	Lett	P	Cittadini/Impr ese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Gestione degli impegni, liquidazione della fatture	dati contabili/dati relativi a fatture e liquidazioni	D/A	Lett- Scrit	P/E	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Gestione atti amministrativi	Dati anagrafici di cittadini/ Imprese identificati nelle delibere determine ed ordinanze	D/A	Lett- Scrit	P	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Gestione Gare ed Appalti	Dati anagrafici delle Imprese o dei Professionisti - Istruttoria delle gara - Casellari Giudiziali	D/A	Lett- Scrit	P	Professionisti / Imprese	Informativa	Sintel / Mepa	Portale	Descritte nel Piano di sicurezza	Regione Lombardia - Consip		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Contratti	Comunicazioni attraverso Posta elettronica	Corrispondenza dell'ufficio	Digitale	Lett- Scrit	P/S/G	Professionisti - Rappresentan te legale Azienda	Informativa	Client Posta	Hosting	Descritte nel GDPR	Associazione Pinamonte - Brianza est		Personale Ufficio / Utenze personali	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessario
Contratti	Anagrafe delle prestazioni Banca dati che raccoglie gli incarichi conferiti dalle pubbliche amministrazioni sia a dipendenti pubblici che a consulenti.	Dati anagrafici delle aziende e dei professionisti	D/A	Lett- Scrit	P	Dipendenti Consulenti	Informativa	PerlaPA	Hosting applicativo	Descritte nel Piano di sicurezza			Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Contratti	Gestione procedimento inerenti la trasparenza amministrativa	Dati anagrafici contabili e tecnici inerenti procedimenti del comune	D/A	Lett- Scrit	P	Dipendenti - Consulenti - Professionisti - Cittadini	Informativa	sessione del sito internet del comune - Portale trasparenza	Hosting applicativo	Descritte nel Piano di sicurezza	Opencontent S.c.a.r.l		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Titolare del Trattamento — Comune di Bellusco - P.zza Fratelli Kennedy 1 - Bellusco — Rappresentante Legale: Sindaco Roberto Invernizzi — Data Aggiornamento 25/05/2018

Responsabile del trattamento — Dott Giorgio Vitali — email comune.bellusco@pec.regione.lombardia.it

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso Dati	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Sportello Unico	Gestione dell'Anagrafe dei Residenti	Dati anagrafici e dati per eventuali comunicazioni	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Ina/SAIA Ministero Interni	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Anagrafe cittadini residenti all'estero	Dati anagrafici	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	ANAG/AIRE Ministero Interni	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Cartellini Carte Identità	Dati anagrafici	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Ministero dell'interno	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Carta identità elettronica	Dati anagrafici , dichiarazione donazione organi	D	Lett- Scrit	P	Cittadini residenti	Informativa	Portale del ministero Interni	Portale del ministero Interni	Descritte nel GDPR		Ministero dell'interno	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	schede di famiglia archiviate in formato cartaceo sino al 2010 e successivamente gestite in formato digitale	Dati anagrafici	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	schede Individuali archiviate in formato cartaceo sino al 2010 e successivamente gestite in formato digitale	Dati anagrafici del nucleo famigliare	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Archivio dello stato civile	Atti di stato civile (Atti di nascita, Atti di matrimonio atti di morte)	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Gestione delle Liste elettorali	Dati anagrafici aventi diritto al voto	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Prefettura - Commissione mandamentale	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Albo scruatori e presidenti di seggio	dati anagrafici	D/A	Lett- Scrit	P/G	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Corte d'Appello	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Fascicoli inibiti al voto	Dati anagrafici inibiti al voto	D/A	Lett	P/G	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Ricevuti dal Tribunale o da altri comuni / trasmissione ad altro comune nel caso di variazione della residenza	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Giudici popolari	dati anagrafici dei giudici popolari	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Tribunale	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Gestione liste di leva	dati anagrafici persone inserite nelle liste che vengono trasmesse al distretto militare	D	Lett- Scrit	P	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Distretto Militare	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Liste anagrafiche comunali	dati anagrafici	D	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Istat	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Statistica Migrazioni ed Immigrazione	Dati aggregati	D/A	Lett- Scrit	P	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Istat - ATS	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Scheda Istat D4 morte	Dati aggregati	D/A	Lett- Scrit	P/S	Cittadini residenti	Informativa	sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	ATS / Prefettura	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Sportello Unico	Gestione cimiteriale Contratti / Loculi	Contratti cimiteriali e dati anagrafici defunto	D/A	Lett- Scrit	P	Cittadini	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Testamento biologico - DAT	dati anagrafici e desideri del soggetto	A	Lett- Scrit	P/S	Cittadini residenti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Corrispondenza in ingresso	Corrispondenza in uscita / e-mail inviate dall'ente attraverso PEC	Digitale ed analogico	Lett- Scrit	P/S/G	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Corrispondenza in uscita	Corrispondenza in ingresso / e-mail inviate all'ente attraverso PEC	Digitale ed analogico	Lett- Scrit	P/S/G	Cittadini - Aziende - Enti	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Atti amministrativi ai sensi del codice di procedura civile	Atti depositati e notificati che vengono depositati presso sede del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA	Regione	Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Gestione depositi atti giudiziari tribunale	Atti depositati e notificati che vengono depositati presso sede del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Gestione notifiche atti tributari	Atti depositati e notificati che vengono depositati presso sede del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Gestione avvisi di deposito dell'agenzia delle entrate presso casa comuale	Atti depositati e notificati che vengono depositati presso sede del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Sicr@web	Server Applicativo	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Pubblicazione Albo pretorio	Dati relativi agli atti amministrativi del comune	Digitale ed analogico	Lett- Scrit	P/S	Cittadini	Informativa	Sito internet del comune	Hosting	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Pubblicazione Amministrazione trasparente	Dati relativi agli atti amministrativi del comune	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Sito internet del comune	Hosting	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Pagamenti servizio mensa	Dati relativi agli utenti del servizio e dati dei geneitori	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Office	File server	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Iscrizione ai servizi scolastici (mensa, trasporto,prescuola	Dati anagrafici , dati componenti nuclo famigliare - attestazione ISEE	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Office	File server	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Iscrizione asilo Nido	Dati anagrafici , dati componenti nuclo famigliare - attestazione ISEE	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Office	File server	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Iscrizione al CRE	Dati anagrafici , dati componenti nuclo famigliare - attestazione ISEE	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Office	File server	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Richiesta contributi socio assistenziali	Dati anagrafici , dati componenti nuclo famigliare - attestazione ISEE	Digitale ed analogico	Lett- Scrit	P	Cittadini	Informativa	Office	File server	Descritte nel GDPR	Maggioli SpA		Personale Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sportello Unico	Comunicazioni attraverso Posta elettronica	Corrispondenza dell'ufficio	Digitale	Lett- Scrit	P/S/G	Professionisti - Rappresentant e legale Azienda	Informativa	Client Posta	Hosting	Descritte nel GDPR	Associazione Pinamonte - Brianza est		Personale Ufficio / Utenze personali	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessario

Titolare del Trattamento | Comune di Bellusco - P.zza Fratelli Kennedy 1 - Bellusco | Rappresentante Legale: Sindaco Roberto Invernizzi | Data Aggiornamento 25/05/2018

Responsabile del trattamento | Dott.ssa Emanuela Ronchi | email comune.bellusco@pec.regione.lombardia.it

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso Dati	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Sociali	Verifica reddituali	Dati reddituali	Digitale	Lett	P	Utenti	Informativa	Punto Fisco	Portale Agenzia Entrate	Descritte nel GDPR		Portale Agenzia Entrate	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Banca Dati casellario dell'Assistenza	Dati relativi ai contributi erogati ai cittadini	Digitale	Lett- Scrit	P	Utenti	Informativa	Portale INPS	Hosting	Descritte nel GDPR		Ministero politiche sociali	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione reddito di inclusione REI	Dati relativi ai contributi e agli interventi di sostegno a favore dell'Utente	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Portale INPS	Hosting	Descritte nel GDPR		INPS	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Cartelle utenti (indigenti , Anziani, Disabili)	Dati utenti e famiglia alunno	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office	file server	Descritte nel GDPR	ATS		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Dati relativi ai contributi Sgate, Energia , Idrico	Dati dei beneficiari importi erogati	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office Portale Sgate	Hosting	Descritte nel GDPR		Portale Ancitel	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Dati relativi ai beneficiari dei contributi di affitto - dati anagrafici, dati relativi alle condizioni economico, famigliari.	Dati dei beneficiari importi erogati	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office	file server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Assegni Maternità	Dati dei beneficiari Stato di salute	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Portale INPS + cartella informatica	Hosting	Descritte nel GDPR		INPS	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Assegni Nucleo Famigliare Numeroso	Dati dei beneficiari importi erogati	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office/Portale Regionale	Hosting	Descritte nel GDPR		INPS	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione contributi utenti RSA	Dati dei beneficiari Stato di salute - Attestazione ISEE	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office	file server	Descritte nel GDPR		RSA	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione pasti a domicilio	Dati dei beneficiari importi erogati. Attestazione ISEE	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office	File Server	Descritte nel GDPR	Ser-CAR		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione servizio Assistenza Domiciliare SAD	Dati degli utenti e Stato di salute, Attestazione ISEE	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office	File Server	Descritte nel GDPR	Cooperativa L'impronta		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione servizio Trasporto sociale	Dati degli utenti e Stato di salute	Digitale ed Analogico	Lett- Scrit	P	Utenti	Informativa	Office	File Server	Descritte nel GDPR	Auser		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Trasporto sociale Disabili	Dati dei beneficiari Stato di salute	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office	File Server	Descritte nel GDPR	Auser		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione Contributi Disabili	Dati dei beneficiari importi erogati. Attestazione ISEE	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office	File Server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione servizio Assistenza Domiciliare SAD per disabili	Dati degli utenti e Stato di salute, Attestazione ISEE	Digitale ed Analogico	Lett- Scrit	P/S	Utenti	Informativa	Office	File Server	Descritte nel GDPR	Coop La persona		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione servizio Assistenza Educativa Scolastica	Dati utenti e relazioni sociali	Digitale ed Analogico	Lett- Scrit	P	Utenti	Informativa	Office	File server	Descritte nel GDPR	Cooperativa L'impronta		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione servizio di tutale minori- Procedure di Affido	Dati dei minori e relazioni sociali	Digitale ed Analogico	Lett- Scrit	P/S/G	Minori	Informativa / Consenso	Office	File Server	Descritte nel GDPR		Ufficio di Ambito -Tribunale	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione contributi famiglia affidataria	Dati dei minori e relazioni sociali	Digitale ed Analogico	Lett- Scrit	P/S	Minori	Informativa / Consenso	Office	File Server	Descritte nel GDPR		Ufficio di Ambito -Tribunale	Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione servizio Assistenza Domiciliare Minori	Dati dei beneficiari importi erogati	Digitale ed Analogico	Lett- Scrit	P/S	Minori	Informativa	Office	File Server	Descritte nel GDPR	Coop L'impronta		Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione associazioni di volontari	Dati volontari	Digitale ed Analogico	Lett- Scrit	P	Utenti	Informativa	Office	File server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Contributi economici alle associazioni	Dati relativi al presidente e ai contributi erogati	Digitale ed Analogico	Lett- Scrit	P	Utenti	Informativa	Office	File server	Descritte nel GDPR			Personale dell'Ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione della corrispondenza in ingresso ed in uscita	Banca dati del protocollo con corrispondenza in entrata ed in uscita	D/A	Lett- Scrit	P	Cittadini / Imprese / altri enti	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Sociali	Anagrafica semplificata dei cittadini e delle Imprese	dati anagrafici	D	Lett	P	Cittadini/Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione degli impegni, liquidazione della fatture	dati contabili/dati relativi a fatture e liquidazioni	D/A	Lett- Scrit	P/E	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione atti amministrativi	Dati anagrafici di cittadini/ Imprese identificati nelle delibere determine ed ordinanze	D/A	Lett- Scrit	P	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione Gare ed Appalti	Dati anagrafici delle Imprese o dei Professionisti - Istruttoria delle gara - Casellari Giudiziali	D/A	Lett- Scrit	P	Professionisti / Imprese	Informativa	Sintel / Mepa	Portale	Descritte nel Piano di sicurezza	Regione Lombardia - Consip		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Comunicazioni attraverso Posta elettronica	Corrispondenza dell'ufficio	Digitale	Lett- Scrit	P/S/G	Professionisti - Rappresentante legale Azienda	Informativa	Client Posta	Hosting	Descritte nel GDPR	Associazione Pinamonte - Brianza est		Personale Ufficio / Utenze personali	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessario
Sociali	Anagrafe delle prestazioni Banca dati che raccoglie gli incarichi conferiti dalle pubbliche amministrazioni sia a dipendenti pubblici che a consulenti.	Dati anagrafici delle aziende e dei professionisti	D/A	Lett- Scrit	P	Dipendenti Consulenti	Informativa	PerlaPA	Hosting applicativo	Descritte nel Piano di sicurezza			Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Sociali	Gestione procedimento inerenti la trasparenza amministrativa	Dati anagrafici contabili e tecnici inerenti procedimenti del comune	D/A	Lett- Scrit	P	Dipendenti - Consulenti - Professionisti - Cittadini	Informativa	sessione del sito internet del comune - Portale trasparenza	Hosting applicativo	Descritte nel Piano di sicurezza	Opencontent S.c.a.r.l		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Titolare del Trattamento — Comune di Bellusco - P.zza Fratelli Kennedy 1 - Bellusco — Rappresentante Legale: Sindaco Roberto Invernizzi — Data Aggiornamento 25/05/2018

Responsabile del trattamento — Rag Giovanna Biella — email comune.bellusco@pec.regione.lombardia.it

Unità Organizzativa - Ufficio	Finalità del trattamento	Tipologia di Dati trattati	Modalità di conservazione dei dati	Diritti Accesso	Classific. Dati	Categorie di interessati	Informativa / Consenso	Software Gestione Archivio	Server Install. DB/Archivio	Regole sicurezza gestione archivio digitale	Responsabile Esterno del Trattamento	Destinatari a cui i dati vengono comunicati i dati	Personale Accesso Dati	Periodo di conservazione dei dati (se possibile)	Paesi Terzi Organizzazioni internazionali verso cui i dati vengono Trasferiti	Effettuazione valutazione di impatto da parte del Titolare
Tributi Locali	Gestione tributo , aggiornamento banca dati, Verifiche ed Accertamenti	Banca Dati TARI - Dati personali die contribuenti	D/A	Lett-Scrit	P	Cittadini Imprese Enti	Informativa	Sicr@web	Hosting presso P.A. digitale	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Gestione tributo , aggiornamento banca dati, Verifiche ed Accertamenti	Banca Dati IMU - Dati personali die contribuenti	D/A	Lett-Scrit	P	Cittadini Imprese Enti	Informativa	Sicr@web	Hosting presso P.A. digitale	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Gestione tributo, aggiornamento banca dati	Banca Dati TASI - Dati personali die contribuenti	D/A	Lett-Scrit	P	Cittadini Imprese Enti	Informativa	Sicr@web	Hosting presso P.A. digitale	Descritte nel GDPR	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Gestione ruoli ed Incassi	Ruoli Coattivi dati degli utenti morosi	D/A	Lett-Scrit	P	Cittadini Imprese Enti	Informativa	Agenzia entrate e riscossioni	Server Applicativo	Descritte nel GDPR		Agenzia Entrate - Riscossioni	Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Consultazione dati Fiscali	Punto Fisco	D	Lett	P/T	Cittadini Imprese Enti	Informativa	Punto Fisco	Server Applicativo	Descritte nel GDPR			Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Consultazione dati Patrimoniali	Agenzia territorio / Sister	D	Lett	P/T	Cittadini Imprese Enti	Informativa	Portale Agenzia Territorio (siatel)	Server Applicativo	Descritte nel GDPR			Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Comunicazione dati al MEF attraverso portale	Dati relativi alle entrate Tributarie	D	Lett	P/T	Cittadini Imprese Enti	Informativa	Portale Federalismo fiscale	Server Applicativo	Descritte nel GDPR	MEF		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Gestione imposta pubblicitaria	Pubblicità e pubbliche affissioni	D/A	Lett-Scrit	P	Cittadini Imprese Enti	Informativa		Server Applicativo	Descritte nel GDPR	**Sarida**		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Consultazione visure camerali	Banca dati camerali	D/A	Lett-Scrit	P	Cittadini Imprese Enti	Informativa	Portale Telemaco	Server Applicativo	Descritte nel GDPR	camera commercio		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Gestione della corrispondenza in ingresso ed In uscita	Banca dati del protocollo con corrispondenza in entrata ed in uscita	D/A	Lett-Scrit	P	Cittadini / Imprese / altri enti	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Anagrafica semplificata dei cittadini e delle Imprese	dati anagrafici	D	Lett	P	Cittadini/Impr ese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Gestione atti amministrativi	Dati anagrafici di cittadini/ Imprese identificati nelle delibere determine ed ordinanze	D/A	Lett-Scrit	P	Cittadini / Imprese	Informativa	Sicr@web	Server Applicativo	Descritte nel Piano di sicurezza	Maggioli SpA		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Gestione Gare ed Appalti	Dati anagrafici delle Imprese o dei Professionisti - Istruttoria delle gara - Casellari Giudiziali	D/A	Lett-Scrit	P	Professionisti / Imprese	Informativa	Sintel / Mepa	Portale	Descritte nel Piano di sicurezza	Regione Lombardia - Consip		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Comunicazioni attraverso Posta elettronica	Corrispondenza dell'ufficio	Digitale	Lett-Scrit	P/S/G	Professionisti - Rappresentant e legale Azienda	Informativa	Client Posta	Hosting	Descritte nel GDPR	Associazione Pinamonte - Brianza est		Personale Ufficio / Utenze personali	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessario
Tributi Locali	Anagrafe delle prestazioni Banca dati che raccoglie gli incarichi conferiti dalle pubbliche amministrazioni sia a dipendenti pubblici che a consulenti.	Dati anagrafici delle aziende e dei professionisti	D/A	Lett-Scrit	P	Dipendenti Consulenti	Informativa	PerlaPA	Hosting applicativo	Descritte nel Piano di sicurezza			Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria
Tributi Locali	Gestione procedimento inerenti la trasparenza amministrativa	Dati anagrafici contabili e tecnici inerenti procedimenti del comune	D/A	Lett-Scrit	P	Dipendenti - Consulenti - Professionisti - Cittadini	Informativa	sessione del sito internet del comune - Portale trasparenza	Hosting applicativo	Descritte nel Piano di sicurezza	Opencontent S.c.a.r.l		Personale dell'ufficio	Vedi Manuale Gestione Documentale	Non Applicabile	Non Necessaria

Comune di BELLUSCO — **ANALISI DEI RISCHI RELATIVA AL TRATTAMENTO DEI DATI** — Data Aggiornamento 25/05/2018

Categoria	Minaccia	Effetto	Proba	effetto	Rischio	Note (giustificazioni per i valori assegnati)	Azioni correttive o Piani di Miglioramento	Persona Incaricata	data di attuazione	Verifica attuazione
Comune Bellusco	Incendio	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Controllo fisici accesso ai locali o Presidio dello stesso Estintori manutenuti da una ditta specializzata Impianto elettrico a norma e controllo Messe a terra Carico incendio non critico				
	Allagamento	Impossibilità di accedere ai locali, danni al Sistema informativo, Danneggiamento dei dati	1	3	3	L'edificio del comune è distante da corsi d'acqua e bacini idrici- Storicità dell'evento bassa				
	Distruzione di strumentazione da parte di persone malintenzionate	Danni al Sistema informativo, Danneggiamento dei dati	1	3	3	Le misure di sicurezza dell'edificio sono adeguate, Storicamente non si sono mai verificati eventi di questo tipo				
	Attacchi Fisici, Furti, Atti vandalici	Danni al Sistema informativo Furto di dati o apparati del SI Danneggiamento dei dati Danno immagine	1	3	3	Il perimetro dell'edificio è coperto da un impianto di Video Sorveglianza Nell'edificio è installato un sistema di allarme Storicamente non si sono mai verificati eventi di questo tipo				
	Fenomeni climatici (Uragani, Nevicate)	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Storicamente non si sono verificati eventi climatici dannosi				
	Terremoti, eruzioni vulcaniche	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Storicamente non si sono verificati eventi naturali dannosi quali terremoti Edificio antisismico o rischio sismico basso				
Biblioteca	Incendio	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Controllo fisici accesso ai locali o Presidio dello stesso Estintori manutenuti da una ditta specializzata Impianto elettrico a norma e controllo Messe a terra Presenza di sensori per rilievo incendi				
	Allagamento	Impossibilità di accedere ai locali, danni al Sistema informativo, Danneggiamento dei dati	1	3	3	L'edificio del comune è distante da corsi d'acqua e bacini idrici- Storicità dell'evento bassa				
	Distruzione di strumentazione da parte di persone malintenzionate	Danni al Sistema informativo, Danneggiamento dei dati	1	3	3	Le misure di sicurezza dell'edificio sono adeguate, Storicamente non si sono mai verificati eventi di questo tipo				
	Attacchi Fisici, Furti, Atti vandalici	Danni al Sistema informativo Furto di dati o apparati del SI Danneggiamento dei dati Danno immagine	1	3	3	Nell'edificio è installato un sistema di allarme Storicamente non si sono mai verificati eventi di questo tipo				
	Fenomeni climatici (Uragani, Nevicate)	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Storicamente non si sono verificati eventi climatici dannosi				
	Terremoti, eruzioni vulcaniche	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Storicamente non si sono verificati eventi naturali dannosi quali terremoti Edificio antisismico o rischio sismico basso				
Sala CED all'interno del palazzo comunale	Incendio	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	2	2	Controllo fisici accesso ai locali o Presidio dello stesso Estintori manutenuti da una ditta specializzata Impianto elettrico a norma e controllo Messe a terra Carico incendio non critico				
	Allagamento	Impossibilità di accedere ai locali, danni al Sistema informativo, Danneggiamento dei dati	1	3	3	L'edificio del comune è distante da corsi d'acqua e bacini idrici- Storicità dell'evento bassa				
	Distruzione di strumentazione da parte di persone malintenzionate	Danni al Sistema informativo, Danneggiamento dei dati	1	3	3	Le misure di sicurezza dell'edificio sono adeguate, Storicamente non si sono mai verificati eventi di questo tipo				
	Attacchi Fisici, Furti, Atti vandalici	Danni al Sistema informativo Furto di dati o apparati del SI Danneggiamento dei dati Danno immagine	1	3	3	Porta Chiusa a chiave Storicamente non si sono mai verificati eventi di questo tipo				
	Fenomeni climatici (Uragani, Nevicate)	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Storicamente non si sono verificati eventi climatici dannosi				
	Terremoti, eruzioni vulcaniche	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Storicamente non si sono verificati eventi naturali dannosi quali terremoti Edificio antisismico o rischio sismico basso				
Archivio documentale	Incendio	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	2	3	6	Estintori manutenuti da una ditta specializzata	Valutare la possibilità di regolamentare l'accesso all'archivio documentale			
	Allagamento	Impossibilità di accedere ai locali, danni al Sistema informativo, Danneggiamento dei dati	1	3	3	L'edificio del comune è distante da corsi d'acqua e bacini idrici- Storicità dell'evento bassa				
	Distruzione di strumentazione da parte di persone malintenzionate	Danni al Sistema informativo, Danneggiamento dei dati	1	3	3	Le misure di sicurezza dell'edificio sono adeguate, Storicamente non si sono mai verificati eventi di questo tipo				
	Attacchi Fisici, Furti, Atti vandalici	Danni al Sistema informativo Furto di dati o apparati del SI Danneggiamento dei dati Danno immagine	1	3	3	Nell'edificio è installato un sistema di allarme Storicamente non si sono mai verificati eventi di questo tipo				
	Fenomeni climatici (Uragani, Nevicate)	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Storicamente non si sono verificati eventi climatici dannosi				
	Terremoti, eruzioni vulcaniche	Impossibilità di accedere ai locali, danni al Sistema informativo, Perdita dei dati	1	3	3	Storicamente non si sono verificati eventi naturali dannosi quali terremoti Edificio antisismico o rischio sismico basso				
Perdita di servizi essenziali inerenti il sistema informativo e la sala server	Guasto aria condizionata o sistemi di raffreddamento	Innalzamento temperatura sala server, Guasto apparati, Blocco Apparati	1	2	2	Impianto di recente installazione Manutenzione periodica				
	Perdita di energia (o sbalzi di tensione)	Guasto ad apparati del sistema informativo Perdita delle sessioni di lavoro	1	2	2	Impianto elettrico a norma e controllo periodico della Messa a terra Presenza batterie continuità Bassa frequenza di Problemi Elettrici				
	Interruzione nei collegamenti di rete (inclusi danni alle linee di TLC)	Mancata accesso a servizi applicativi Difficoltà di comunicazione con soggetti esterni	1	2	2	Connessione dati ridondata Contratto assistenza con definizione SLA Bassa Frequenza di Problemi con le reti TLC				
	Interruzione del servizio di posta elettronica	Mancata accesso a servizi applicativi Difficoltà di comunicazione con soggetti esterni Mancata erogazione servizi agli utenti	1	2	2	Connessione dati ridondata Contratto assistenza con definizione SLA Bassa Frequenza di Problemi con le reti TLC				
	Interruzione del servizio di hosting dei dati o delle applicazioni in cloud	Mancata accesso a servizi applicativi Difficoltà di comunicazione con soggetti esterni Mancata erogazione servizi agli utenti	1	2	2	Connessione dati ridondata Contratto assistenza con definizione SLA Bassa Frequenza di Problemi con le reti TLC				
	Eccesso di traffico sulla rete	Mancata accesso a servizi applicativi Difficoltà di comunicazione con soggetti esterni Mancata erogazione servizi agli utenti	1	2	2	Apparati di rete di recente installazione Presenza di sistemi di protezione della Rete IL comune sta valutando l'acquisto di uno strumento per il monitoraggio della rete				
	Interruzione di servizi erogati riconducibili ai fornitori esterni	Mancata accesso a servizi critici Impossibilità di erogare servizi agli utenti/ fornitori	1	2	2	Fornitori utilizzati sono stati selezionati Progettazione dei servizi critici ha valutato il rischio associato				
	Disturbi elettromagnetici	Guasto ad apparati del sistema informativo	1	2	2	Apparati di rete di recente installazione Presenza di sistemi di protezione della Rete Assenza di elementi di disturbo (impianti industriali con carichi induttivi)				
	Polvere, corrosione	Guasto ad apparati del sistema informativo, Surriscaldamento degli apparati	1	2	2	Non Sono attuate periodiche e cadenzate attività di pulizia e manutenzione dei server degli apparati di rete e degli apparati citrici Gli apparati di rete installati ai vari piani degli edifici del comune sono chiusi negli armadi				
	Ricezione dati da origini non affidabili	Danno al sistema informativo, Danno alle banche dati,	1	2	2	La rete del comune NON è protetta da apparato di protezione perimetrale Posta elettronica ha attivato un Tool antispam Sulle postazioni di lavoro è installato sw antivirus Viene fatta scansione periodica delle PDL	valutare la necessità di installare un apparato di protezione perimetrale con funzioni avanzate di sicurezza per la rete (IPS antivirus ecc.)			

1	Sicurezza della Rete	Infiltrazione nelle comunicazioni	Furto di dati, Codici, Violazione della Privacy	1	2	2	La rete del comune NON è protetta da apparato di protezione perimetrale	valutare la necessità di installare un apparato di protezione perimetrale con funzioni avanzate di sicurezza per la rete (IPS antivirus ecc.)				
1							Controllo delle postazioni di lavoro tramite antivirus					
1							Controllo dei server con software antivirus					
1		Ripudio dei messaggi	Alterazione delle banche dati e dei messaggi	1	2	2	I portali usano sistemi sicuri di trasmissioni delle informazioni					
1		Possibilità di intrusioni ed accessi non autorizzati all'interno della rete locale e dei server, dovuti a scarsa efficacia della protezione fornita dal firewall	Furto di dati, blocco dei sistemi informativi	1	2	2	Monitoraggio dei log del Router					
1												
1							Sono stati attivati i firewall personali delle PDL					
1							Il software antivirus rileva alterazioni delle configurazioni del computer					
1		Possibilità di installare sw non autorizzato	Danno alla rete informatica, danno alle banche dati, cattivo funzionamento degli apparati di elaborazione	1	3	3	Gli utenti delle PDL non sono amministratori della postazione di lavoro	IL comune sta valutando l'acquisto di uno strumento per il monitoraggio della rete				
1							Antivirus controlla eventuali modifiche al registro del Computer					
1							I codici di autenticazione degli utenti amministrativi sono gestiti con delle policy che prevedono l'uso di password forti e codici identificativi univoci					
1		Accesso non autorizzato alla rete (anche tramite AP wireless non autorizzati)	Danno alla rete informatica, danno alle banche dati, cattivo funzionamento degli apparati di elaborazione	1	2	2	Accesso alla rete tramite dominio					
1							Regole di autenticazione gestite tramite dominio					
1							Non esistono reti ad accesso pubblico					
1		Impossibilità o difficoltà nel ripristinare le configurazione della rete o degli accessi al web	Danno alla rete informatica, danno alle banche dati, cattivo funzionamento degli apparati di elaborazione	1	2	2	Backup del dominio di rete					
1							Backup delle macchine virtuali					
1							Backup delle configurazioni del firewall					
1							Backup delle configurazioni del proxy					
1	Hardware	Possibilità di danneggiare o mettere fuori uso le risorse hardware.	Impossibilità di utilizzare del sistema informativo	1	2	2	Gli apparati di rete installati ai vari piani degli edifici del comune sono chiusi negli armadi					
1							Sistema di Allarme					
1							Uffici vengono chiusi					
1							Apparati di rete chiusi in armadi dotati di serratura					
1		Furto di apparati o componenti	Impossibilità di utilizzare del sistema informativo	1	2	2	Accessi sala server regolamentati e presenza di accessi protetti					
1							Sistema di Allarme					
1							Uffici vengono chiusi					
1							Apparati di rete chiusi in armadi dotati di serratura					
2		Possibilità di asportare/manomettere unità di memoria Removibile	Furto di dati, predita di dati divulgazione di dati	1	2	2	Le unità di memoria sono conservate in luoghi sicuri					
2							La sostanza che contiene i server è chiusa a chiave					
2							La stanza in cui vengono conservate le unità di memoria sono allarmate					
2		Fault o malfunzionamento della strumentazione IT	Impossibilità di utilizzare del sistema informativo	1	2	2	Apparati Alimentati da batterie di Continuità					
2							Apparati di recente Installazione					
2							Apparati di Classe Enterprise					
	SW	Malfunzionamenti software di Base	Errore di elaborazione - Blocco del sistema informativo	1	2	2	Il software di base si aggiorna automaticamente sulle PdL					
							Il software di base si aggiorna automaticamente sui server					
							Il comune ha installato un software antivirus					
							Assenza Procedura di Collaudo					
		Malfunzionamenti software Applicativi usati dai vari uffici	Inefficienza del settore che utilizza l'applicazione, Impossibilità di accedere alla banca dati	1	2	2	Qualità software buona					
							Fornitore affidabile dotato di sistema di gestione della qualità					
		Recupero di informazioni da media (principalmente memorie di massa) dismessi.	Violazione della Privacy Diffusione di informazioni riservate Danno di Immagine	1	2	2	Corretta gestione dei supporti					
							Consapevolezza nella gestione dei supporti					
							Furto dei supporti di memorizzazione					
	DATI	Perdita di documenti Archivio Documentale	Violazione della Privacy Diffusione di informazioni riservate - Perdita dei documenti originali - Inefficienza nella gestione dell'attività	1	2	2	Conservazione dei supporti di memorizzazione in luoghi sicuri					
							I documenti dell'archivio cartaceo vengono custoditi in armadi/cassetti chiusi a Chiave					
		Perdita di documenti Archivio Biblioteca	Violazione della Privacy Diffusione di informazioni riservate - Perdita dei documenti originali - Inefficienza nella gestione dell'attività	1	2	2	Accesso alle banche dati gestito correttamente					
							I documenti dell'archivio cartaceo vengono custoditi in armadi/cassetti chiusi a Chiave					
		Perdita di documenti Archivio Demografico	Violazione della Privacy Diffusione di informazioni riservate - Perdita dei documenti originali - Inefficienza nella gestione dell'attività	1	2	2	Accesso alle banche dati gestito correttamente					
							I documenti dell'archivio cartaceo vengono custoditi in armadi/cassetti chiusi a Chiave					
		Perdita di documenti Archivio Ragioneria	Violazione della Privacy Diffusione di informazioni riservate - Perdita dei documenti originali - Inefficienza nella gestione dell'attività	1	2	2	Accesso alle banche dati gestito correttamente					
							I documenti dell'archivio cartaceo vengono custoditi in armadi/cassetti chiusi a Chiave					
		Perdita di documenti Archivio Servizi sociali	Violazione della Privacy Diffusione di informazioni riservate - Perdita dei documenti originali - Inefficienza nella gestione dell'attività	1	2	2	Accesso alle banche dati gestito correttamente					
							I documenti dell'archivio cartaceo vengono custoditi in armadi/cassetti chiusi a Chiave					
		Distruzione/Danneggiamento dei file Office a causa di Virus (malware, anche per mobile)	Perdita di dati	1	2	2	Il personale è stato formato sulle modalità e causa di diffusione dei virus					
			Difficoltà nell'erogare servizi agli utenti				L'organizzazione ha installato un software antispam					
			Inefficienza legata alla necessità di ripristinare gli apparati di elaborazione				L'organizzazione ha installato un software antivirus professionale					
			Danno economico				L'organizzazione ha definito delle policy di configurazione dell'antivirus	Valutare la necessità di programmare la scansione completa delle PdL				
			Danno di Immagine				L'organizzazione NON ha installato un apparato che filtra l'accesso ai siti web	Valutare l'opportunità di attivare un Tool che gestisce gli accessi ad internet				
		Distruzione/Danneggiamento dei Data Base degli applicativi di business a causa di Virus	Perdita di dati	1	1	1	Il personale è stato formato sulle modalità e causa di diffusione dei virus					
			Difficoltà nell'erogare servizi agli utenti				L'organizzazione ha installato un software antispam					
			Inefficienza legata alla necessità di ripristinare gli apparati di elaborazione				L'organizzazione ha installato un software antivirus professionale					
			Danno economico				L'organizzazione ha definito delle policy di configurazione dell'antivirus					
			Danno di Immagine				L'organizzazione ha definito delle policy di configurazione dell'antivirus	Valutare la necessità di programmare la scansione completa delle PdL				
							L'organizzazione NON ha installato un apparato che filtra l'accesso ai siti web	Valutare l'opportunità di attivare un Tool che gestisce gli accessi ad internet				
		Trattamento (volontario o inconsapevole) non consentito di dati (personali)	Diffusione di dati	1	1	1	L'organizzazione ha profilato l'accesso alle banche dati					
			Accesso non consentito e violazione regole di profilazione				L'organizzazione ha profilato l'accesso alle cartelle del file server					
			Possibile perdita di dati				I dati vengono salvati nella cartelle del server					
		Cancellazione/modifica non autorizzata alle risorse dati in formato elettronico.	Diffusione di dati	1	1	1	Accesso alla rete o alle PDL avviene tramite id e password					
			Accesso non consentito e violazione regole di profilazione				L'organizzazione ha profilato l'accesso alle banche dati					
			Possibile perdita di dati				L'organizzazione ha profilato l'accesso alle cartelle del file server					
		Incapacità o difficoltà a ripristinare copie di backup	Perdita di dati, difficoltà nel ripristinare funzionamento del sistema informativo	1	3	3	Backup vengono fatti su diversi supporti					
							Attivo servizio di backup geografico					
							Periodo di retention 5 giorni	Valutare l'opportunità di creare una struttura virtuale dei server critici				
							Periodicamente vengono fatte delle prove di restore dei dati	Formalizzare le prove che vengono effettuate				
		Difficoltà ad accedere ai dati tempestivamente in caso di situazioni di emergenza.	Mancata erogazione del servizio	1	1	1	Dati importanti sono salvati su server in cartelle profilate					
			Inefficienza				La password di amministratore di sistema è gestita correttamente					
			danno di immagine				L'organizzazione ha impostato delle policy di backup dei dati					
		Rischi derivanti dalla mancata pseudonimizzazione dei dati o Criptazione riguardanti lo stato di salute e la vita sessuale.	Diffusione di dati sensibili	1	1	1	L'organizzazione NON utilizza strumenti di criptazione dei dati sensibili					
			Non ottemperanza alla normativa relativamente alla data protection				L'organizzazione NON utilizza tecniche di speudonizzazione	Attivare delle procedure per la gestione corretta dei dati sensibili				
			non corretta gestione del dato da parte di soggetti esterni				E stata fatta una mappatura dei dati inerenti lo stato di salute e sono state adottate policy che restringono all'accesso a queste informazioni					
		Rischi derivanti dalla mancata separazione dei dati (in formato cartaceo) riguardanti lo stato di salute e la vita sessuale.	Diffusione di dati sensibili				I dati sensibili sono custoditi in armadi chiusi a chiave					
			Non ottemperanza alla normativa relativamente alla data protection				Il personale chiude gli uffici nei quali sono archiviati i dati sensibili					
			non corretta gestione del dato da parte di soggetti esterni				I sdati sensibili sono custoditi in busta chiuse e sigillate					
		Indisponibilità di personale (malattie, sciopero, eccetera)	Difficoltà nell'erogare servizi agli utenti	1	1	1	I dati sono salvati su server in modo che possano essere accessibili al ufficio					
			Inefficienza				le mansioni sono distribuite su persone diverse					
		Errori degli utenti del sistema informativo	Cancellazione Perdita danneggiamento involontario dei dati	1	1	1	Il personale è qualificato					
			mancata attuazione del principio di integrità nell'accesso alle banche dati				Prima di intraprendere un attività / mansione il personale viene addestrato	Formalizzare i piani di formazione / Affiancamento				

		danneggiamento a causa di virus informatici				L'accesso alle banche dati digitali è profilato					
	Uso dei servizi da parte di persone non autorizzate o elevamento di privilegi.	Cancellazione Perdita danneggiamento involontario dei dati	1	1	1	Accesso alle rete / Postazioni di lavoro avviene tramite Id e password					
		mancata attuazione del principio di integrità nell'accesso alle banche dati				L'accesso alle banche dati digitali è profilato					
	Degrado dei media (memorie di massa)	Perdita di dati	2	2	4	I supporti di memorizzazione soggetti a degrado vengono periodicamente sostituiti					
		Impossibilità di ripristinare le copie di sicurezza				Il salvataggio delle banche dati avviene su dispositivi di classe enterprise					
Compromissione di funzioni	Rivelazione di informazioni (da parte del personale o fornitori)	Non corretta gestione dei dati				I fornitori che gestiscono le banche dati vengono qualificati					
		Non corretta attuazioni delle prescrizioni normative	2	2	4	Il fornitore viene incaricato responsabile del trattamento dei dati					
		Diffusione comunicazione non corretta dei dati				Al fornitore vengono chieste delle evidenze sulle policy relative al trattamento dei dati					
	Furto identità	Accesso non autorizzato ai dati				L'accesso alle banche dati digitali è profilato					
		Esecuzione di operazione senza la tracciabilità delle stesse				Accesso alle rete / Postazioni di lavoro avviene tramite Id e password					
		Esecuzioni di operazioni non consentite	2	2	4	La gestione delle utenze amministrative NON rispetta le indicazioni della circolare AGID	Modificare la gestione delle utenze amministrative come indicato nella circolare Agid n2 2017				
		Accesso ai servizi di portale da parte di persone non autorizzate				Non sempre l'accesso ai portali esterni avviene tramite codici di autenticazione personali	Attivare la procedura per la gestione delle utenze a servizi esterni				
		Diffusione di dati				I servizi di portale rivolti hai cittadini usano delle policy di autenticazione corretta					
		Inconsapevole danneggiamento alle banche dati				L'accesso alla rete di internet da parte degli utenti è protetta da un antivirus con funzione di protezione da siti malevoli					
		Danni a causa di attività di fishing o ingegneria sociale				I servizi di portale rivolti hai cittadini usano delle policy di autenticazione corretta					
1	Rischi di trattamenti non corretti e non conformi dovuti alla mancata redazione di norme e istruzioni scritte e dettagliate ad uso degli incaricati del trattamento dei dati.	Sanzioni da parte delle autorità competenti, Reclami da parte degli interessati	1	1	1	E' stato definito un regolamento in materia di data Protection	Il regolamento deve essere adottato				
						Sono stati definiti ruoli e responsabilità					
						Il personale ha acquisito consapevolezza nel trattamento dei dati					
						Sono stati fatte delle attività di formazione e sensibilizzazione					
						Vengono periodicamente condotti degli Audit per verificare la corretta gestione della data protection e dell'attuazione delle normative di legge					
1	Non corretta definizione dei ruoli e delle responsabilità nella gestione dei dati	Mancata attuazione delle procedure di trattamento die dati	1	1	1	Sono stati definiti ruoli e responsabilità	Devono essere fatte le nomine del personale esterno ed interno che tratta dati				
						L'organizzazione ha identificato i responsabili sw trattamento dei dati	Devono essere fatte le nomine del personale esterno ed interno che tratta dati				
						L'organizzazione ha identificato la figura del responsabile della protezione dei dati					
1	Rischi di sanzioni dovuti alla mancata nomina e responsabilizzazione dell'Amministratore di Sistema.	Sanzioni da parte delle autorità competenti - danno di immagine . Non corretta gestione dei dati - non rispetto delle prescrizioni normative	1	1	1	La nomina dell'amministratore è stata formalizzata					
						Le utenze amministrative sono gestite come indicato nel procedimento del Garante e nella circolare AGID sulle misure minime di sicurezza					
						L'organizzazione gestisce il logging delle utenze amministrative					
						I codici di autenticazione delle utenze amministrative rispettano le indicazioni della direttiva Agid relativa alle misure minime di sicurezza					
Rischio Sanzioni per non ottemperanza alle Normative e Leggi Cogenti	Rischi di sanzioni a causa della mancata notificazione al Garante del Data Breach	Sanzioni da parte delle autorità competenti - danno di immagine	1	1	1	E' stata definita una procedura inerente la gestione della data Breach					
						Il personale dell'organizzazione ha acquisito consapevolezza sulla procedura da seguire	è stato programmato un piano di formazione				
	Rischi di sanzioni e trattamenti non conformi dovuti alla mancata individuazione e nomina delle aziende e del personale esterno coinvolto nel processo di trattamento dei dati.	Sanzioni da parte delle autorità competenti - danno di immagine . Non carretta gestione dei dati da parte dei Soggetti esterni	1	2	2	I fornitori sono stati qualificati in relazione all'attività di trattamento die dati					
						Nei confronti dei fornitori sono stati attuati sottoscritti dei contratti ma NON sono state definite le regole di gestione dei dati	Devono essere fatte le nomine del personale esterno ed interno che tratta dati				
						Periodicamente vengono fatte delle verifiche e degli audit sulla attuazione delle policy di data protection					
	Rischi di sanzioni per la non corretta acquisizione del consenso al trattamento dei dati	Sanzioni da parte delle autorità competenti, Reclami da parte degli interessati	1	2	2	Il personale dell'organizzazione ha acquisito consapevolezza sulla procedura da seguire					
						Vengono fatte delle verifiche periodiche sulla gestione del processo di acquisizione del consenso					
						Vengono fatte delle verifiche periodiche sulla gestione del processo di acquisizione del consenso dei portali usati dall'organizzazione					
						Il personale dell'organizzazione è stato informato sulle policy di gestione dei dati	è stato programmato un piano di formazione				
	Rischi di sanzioni per la non corretta gestione dell'Informativa	Sanzioni da parte delle autorità competenti	1	2	2	Il personale dell'organizzazione ha acquisito consapevolezza sulla procedura da seguire					
		Reclami da parte degli interessati				Vengono fatte delle verifiche periodiche sulla gestione del processo di acquisizione del consenso					
		Mancata comunicazione delle policy inerenti l'uso delle risorse del SI				Vengono fatte delle verifiche periodiche sulla gestione del processo di acquisizione del consenso dei portali usati dall'organizzazione					
		Mancata comunicazione delle policy inerenti le attività di controllo sull'uso delle risorse del SI				Il personale dell'organizzazione è stato informato sulle policy di gestione dei dati	è stato programmato un piano di formazione				