Comune di Caravaggio
Provincia di Bergamo

DOCUMENTO ORGANIZZATIVO PER LA PROTEZIONE DEI DATI PERSONALI

redatto ai sensi del Regolamento UE n. 2016/679 e del d. lgs. n. 196 del 2003, c.d. "Codice della Privacy", così come modificato dal d. lgs. n. 101 del 2018

Sommario

1. INTRODUZIONE

Lo scopo del presente Documento è:

1) delineare le misure tecniche e organizzative messe in atto sin dalla progettazione del trattamento, al fine garantire la corretta applicazione dei principi relativi al trattamento dei dati personali. Tali principi riguardano:

   a) Liceità, correttezza e trasparenza
   b) Limitazione della finalità
   c) Minimizzazione dei dati
   d) Esattezza
   e) Limitazione della conservazione
   f) Integrità e riservatezza
   g) Responsabilizzazione

   Nell'individuare le misure suddette, l'Ente ha garantito che siano trattati per impostazione definita solo i dati personali necessari per ogni specifica finalità del trattamento. Inoltre, sempre per impostazione definita, sono state predisposte le misure per limitare la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

2) dimostrare che il trattamento è effettuato conformemente alle disposizioni in materia di trattamento dei dati personali.

Le eventuali incongruenze, che dovessero essere accertate rispetto a quanto precisato nel presente Documento, dovranno essere rimosse nel più breve tempo possibile.
Il presente Documento rimane valido finché non intervengano delle circostanze idonee ad apportare delle variazioni nei processi di trattamento dei dati personali.
IN tale evenienza, il presente Documento dovrà essere immediatamente aggiornato e portato a conoscenza del personale.

2. CONCETTI, DEFINIZIONI E NORMATIVA DI RIFERIMENTO

Principali definizioni normative

(art. 4 Regolamento Ue)

dato personale	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
trattamento	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
profilazione	qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
pseudonimizzazione	il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
archivio	qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
titolare del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
destinatario	la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
terzo	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile
consenso dell'interessato	qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
violazione dei dati personali	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
dati genetici	i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
dati biometrici	i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

dati relativi alla salute	i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
stabilimento principale	a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
rappresentante	la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
impresa	la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
gruppo imprenditoriale	un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
norme vincolanti d'impresa	le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
autorità di controllo	l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;
autorità di controllo interessata	un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;
trattamento transfrontaliero	a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
obiezione pertinente e motivata	un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi

	posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
servizio della società dell'informazione	il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);
organizzazione internazionale	un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.
Altre Definizioni o specificazioni	
Sub-responsabile del trattamento:	il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo), a cui il Responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento di dati personali svolte per conto del Titolare. Il ricorso al Sub-responsabile deve essere preventivamente autorizzato per iscritto da quest'ultimo.
Delegato dal Titolare del trattamento – Referente interno privacy:	figura facoltativa, a cui il Titolare può ricorrere a fini meramente organizzativi.
Garanzie per il trasferimento dei dati in un Paese extra UE:	decisione di adeguatezza della Commissione europea, norme vincolanti d'impresa, clausole contrattuali standard, codice di condotta, meccanismo di certificazione, clausole ad hoc autorizzate dal Garante privacy. In via residuale e in mancanza di una decisione di adeguatezza ovvero delle altre citate garanzie, il trasferimento è ammesso, tra l'altro, se l'interessato vi abbia esplicitamente acconsentito oppure se lo stesso trasferimento sia necessario all'esecuzione di un contratto concluso con il titolare o a tra questi e un terzo a favore dell'interessato. Per maggiori informazioni sulle ulteriori condizioni per il trasferimento dei dati extra UE, v. art. 49 GDPR.

Principali riferimenti normativi

Regolamento Europeo – 2016/679	**Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016**
Decreto legislativo del 30 giugno 2003, n. 196 e s.m.i	Codice in materia di protezione dei dati personali e successive modificazioni e integrazioni
Decreto Legislativo 10 agosto 2018, n. 101	Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018)
Normative comunitarie	
Dir. CE 24 ottobre 1995, n. 46	Direttiva del Parlamento Europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati.
Dir. CE 15 dicembre 1997, n. 66	Direttiva del Parlamento Europeo e del Consiglio sul trattamento di dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni.

Dir. CE 12 luglio 2002, n. 58	Direttiva del parlamento Europeo e del Consiglio relativa al trattamento di dati personali ed alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata ed alle comunicazioni elettroniche).
Commissione Europea – Bruxelles 25 gennaio 2012	Proposta di Regolamento del Parlamento Europeo e del Consiglio – concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei dati.
Provvedimenti dell'Autorità Garante	
Provvedimento 1° Marzo 2007	Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori in ambito privato.
Provvedimento 27 novembre 2008	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
Provvedimento 8 aprile 2010	Disciplina in materia di videosorveglianza.
Provvedimento 19 gennaio 2011	Prescrizioni per il trattamento di dati personali per finalità di marketing, mediante l'impiego del telefono con operatore a seguito dell'istituzione del registro pubblico delle opposizioni (d.p.r. n.178/2010).
Provvedimento 8 maggio 2014	Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie.
Provvedimento n. 245 del 15 maggio 2014	Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati.
Provvedimento Anac n. 1309 del 28 dicembre 2016	Linee guida recanti indicazioni operative i fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d. lgs. n. 33/2013
Provvedimento Anac n. 1310 del 28 dicembre 2016	Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. 33/2013 come modificato dal d.lgs. 97/2016.
Privacy Shield	Accordo che regolamento il trasferimento di dati tra Unione europea e Usa.
Normative internazionali	
l. 21 febbraio 1989, n. 98	Ratifica ed esecuzione della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981.
Carta di Venezia del 30 settembre 2000	Dichiarazione sottoscritta da 28 Paesi, nei quali esiste un'Autorità Garante per la protezione dei dati personali.

Le istruzioni organizzative e tecniche descritte nel presente documento sono verificate e aggiornate dai Titoli di posizione organizzativa, in quanto designati autorizzati dal Titolare del trattamento con specifici compiti e funzioni (vedi Decreti sindacali), coadiuvato dai designati autorizzati al trattamento.
Sarà necessario, quindi, procedere ad una attenta rilettura, nonché all'aggiornamento dello stesso ogni qualvolta si verifichi almeno una delle seguenti condizioni:

- evoluzione del contesto normativo e legislativo di riferimento;
- modifiche organizzative privacy aziendali;
- introduzione di nuovi trattamenti;
- modifiche all'infrastruttura del sistema informativo preposto al trattamento dei dati personali;
- ulteriori e nuovi rischi nell'evoluzione tecnica e tecnologica.

A tal fine, il Titolare verificherà periodicamente, anche coadiuvato dai responsabili, ciascuno per l'area di competenza, sullo stato dei trattamenti in essere e sulle misure di sicurezza in atto, e, una volta valutata la conseguente necessità, provvederà, secondo l'ambito di incidenza (normativo e/o aziendale etc.), agli

aggiornamenti inerenti, in relazione al caso, le procedure, le nomine, oltreché i trattamenti e le istruzioni organizzative e tecniche.

3. ORGANIGRAMMA

3.1. Dati del titolare del trattamento

Titolare del trattamento dei dati personali è il **COMUNE DI CARAVAGGIO**, in persona del legale rappresentante.

Tramite l'adozione di appositi atti, il Titolare ha delegato alcuni compiti ai sotto elencati soggetti, che per esperienza, capacità e affidabilità possono garantire il pieno rispetto delle vigenti disposizioni in materia di tutela della privacy, ivi compreso il profilo della sicurezza, negli ambiti di rispettiva competenza organizzativa:

Area 1 – MAGGIONI Maria Elisa
Area 2 – COSTA Clara
Area 3 – FAGIOLI Claudia
Area 4 – BORDEGARI Paolo
Area 5 – DONIN Massimo
Area 6 – MORONI Paola
Area 7 – RUGGERI Federica
Area 8 –VASSALLI Cristiana

Tutte le misure adottata dall'Area 7 – Farmacia comunale – in materia di trattamento dei dati personali, di gestione della sicurezza delle informazioni, di gestione dei processi di conformità e delle relazioni contrattuali sono gestite con il software "Pharmaprivacy" ed il pacchetto "Servizi Team System Support Gruppo PHS della soc. Pharmaservice s.r.l., con sede in via Cicolella 18 - Lecce.

3.2 Responsabile della protezione dei dati

Artt. 37 - 39 Regolamento UE 2016/679

Responsabile della Protezione dei Dati è il Dott. Filippo Paradiso, il Segretario Generale del Comune di Caravaggio (BG) con sede in Piazza Garibaldi, 9 - Telefono: 0363356202

Il responsabile della protezione dei dati è stato nominato ai sensi dell'art. 37 del Regolamento UE 2016/679 ed è stato incaricato a svolgere almeno i seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dall'applicazione della normativa;
b) sorvegliare l'osservanza della normativa Privacy,
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l 'autorità di controllo per questioni connesse al trattamento.

I dati di contatto sono:

3.3 Designati autorizzati al trattamento

Art. 29 Regolamento UE 2016/679

Il trattamento dei dati personali è consentito alle persone debitamente autorizzate, al solo fine di adempiere ai compiti che gli sono stati assegnati con specifico incarico.
Le persone autorizzate al trattamento sono i soggetti che operativamente effettuano i trattamenti e sono individuate tramite l'assegnazione alla struttura organizzativa di competenza delle persone autorizzate con delega. Ad essi vengono fornite le istruzioni per il trattamento dei dati personali.

Persone autorizzate al trattamento	All. 1 alla cartella n. 1 del Modello Organizzativo di ciascuna Area – Tabella autorizzati

3.4 Responsabili del trattamento

Art. 28 Regolamento UE 2016/679

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre 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.
2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

3.5. Amministratori Di Sistema

Sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi è affidato spesso anche il compito di vigilare sulla protezione dei sistemi informatici di un'azienda o di una pubblica amministrazione
Il Titolare del trattamento si avvale della figura di Amministratore di Sistema, che ha il compito di:

- gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza della Società;
- gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
- monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
- creare, modificare, rimuovere o utilizzare qualunque account o privilegio purché rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati

- rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché rientranti nelle normali attività di manutenzione, gestione della sicurezza, e della protezione dei dati;
- provvedere alla sicurezza informatica dei sistemi informativi aziendali,
- utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata ad un Utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso.

Elenco responsabili del trattamento dati	All. 2 alla cartella n. 1 del Modello Organizzativo di ciascuna Area – Tabella Responsabili del trattamento dati

4. TRATTAMENTI EFFETTUATI

Art. 30 Regolamento UE 2016/679

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà

dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Registro della attività di trattamento	All. 3 alla cartella n. 1 del Modello Organizzativo di ciascuna Area – Registro delle attività trattamento

5. MISURE DI SICUREZZA

Art. 32 Regolamento Europeo 2016/679

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.
4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati
membri.

Nei documenti allegati a) e b) al Registro delle attività di trattamento sono descritte le misure tecniche e organizzative adottate dall'Ente e sono messe in relazione ai principali rischi che gravano in modo trasversale su tutte le operazioni di trattamento dati.
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:

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

- Errori umani
- Guasti alle apparecchiature

Una volta identificati i possibili fattori di rischio associato alle diverse parti del sistema di gestione dei dati personali, 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. La valutazione è stata fatta tenendo conto degli obiettivi della sicurezza informatica:

- Riservatezza
- Integrità
- Disponibilità

La valutazione del rischio residuo è indicata per ogni processo nel Registro delle attività di trattamento, utilizzando i livelli BASSO – MEDIO – ALTO.

Misure di sicurezza	All. a) e b) al Registro delle attività trattamento predisposto da ciascuna Area (cartella n. 1 del Modello Organizzativo)