Allegato 1)

Schema di Regolamento comunale per l'attuazione del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Allegati

A) schema di registro attività di trattamento
B) schema di registro categorie di attività di trattamento

Art. 1.

Oggetto

1. Il presente Regolamento ha per oggetto l'adozione delle misure procedimentali e delle regole necessarie per dare attuazione al Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Montevarchi .

Art. 2.

Titolare del trattamento

1. Il Comune di Montevarchi, rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

2. Il Titolare determina le finalità e i mezzi del trattamento di dati personali e decide sul profilo della sicurezza.

3. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

4. Il Titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato in modo conforme al RGDP. Il Titolare deve verificare e aggiornare dette misure qualora necessario.

5. Le misure sono definite dal Titolare fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato, così come descritti dagli articoli da 15 a 22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

6. Ai sensi dell'art. 35 RGPD, nel caso in cui un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, in particolare se prevede l'uso di nuove tecnologie, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito "DPIA"). Qualora la DPIA indichi che il trattamento presenti un rischio elevato in assenza di misure adottate dal Titolare per attenuarne il rischio, Questi, prima di procedere al trattamento, consulta l'autorità di controllo.

7. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione,

del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

8. Il Titolare sceglie consapevolmente i soggetti che ricoprono i ruoli subalterni e li istruisce. Provvede a:

a) designare i Responsabili del trattamento nelle persone degli apicali preposti alle singole strutture (dirigenti e/o p.o.) in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

b) nominare il Responsabile della protezione dei dati, scegliendolo tra i soggetti che hanno esperienza e professionalità giuridica, anche sotto il profilo applicativo;

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

d) predisporre, in relazione alle dimensioni organizzative del Comune, l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

e) fornisce istruzioni adeguate al personale che tratta i dati

9. Nel caso di violazione dei dati personali deve porre in essere contromisure effettive e tempestive e procedere alla notificazione al Garante ai sensi dell'art. 33 RGDP e, nei casi previsti, alla comunicazione all'interessato ai sensi dell'art. 34 RGDP.

10. Il Titolare adotta misura appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

Successivamente, si dota di idonea organizzazione per riscontrare tempestivamente le istanze dell'interessato e per permettere l'esercizio dei diritti riconosciuti così come esposto all'art. 2.5 del presente Regolamento.

11. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato,

e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

12. Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art.3

Finalità del trattamento

1. I trattamenti sono compiuti dal Comune di Montevarchi per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

- l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
- la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina.

b) l'adempimento di un obbligo legale al quale è soggetto il Comune.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

c) l'esecuzione di un contratto con soggetti interessati;

d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 4

Responsabile del trattamento

1. Il Titolare può avvalersi, per il trattamento di dati, anche di quelli descritti dagli artt. 9 e 10 RGPD, di soggetti pubblici o privati che, in qualità di Responsabili del trattamento forniscano le garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità per mettere in atto le misure tecniche e organizzative di cui all'art. 6 al fine di garantire che i trattamenti siano effettuati in conformità al RGPD, stipulando atti giuridici in forma scritta, che specifichino la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

2. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28.3 RGPD. Tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

3. I dipendenti del Comune, Responsabili del trattamento, sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun Responsabile designato.

4. L'atto giuridico con cui il Titolare effettua la nomina deve prevedere, in particolare, quanto previsto dall'art. 28 RGPD; nello specifico deve prevedere che il Responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, secondo quanto specificato dall'art. 28.3 lett. a) RGPD;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'art. 32 RGPD;

d) rispetti le condizioni di cui agli artt. 28.2 e 28.4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del RGPD;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 RGPD, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del Titolare, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, così come descritto dall'art. 28.3 lett. g) RGPD;

h) metta a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 RGPD e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare o da un altro soggetto da Questi incaricato.

5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che

legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.
Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.
6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
a) alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;
b) all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
c) alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
d) alla eventuale designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
e) ad assistere il Titolare nella conduzione DPIA fornendo allo stesso ogni informazione di cui è in possesso;
f) ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach") per la successiva notifica della violazione al Garante Privacy, disciplinata dall'art. 33 RGPD.

Art. 5
Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con DPO o RPD) è individuato o nella figura di un dipendente di ruolo del Comune, ovvero di un professionista scelto tramite procedura ad evidenza pubblica.
2. Il RPD è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'art. 39 RGPD.

3. Ai sensi dell'art. 39 RGPD, il RPD è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla DPIA e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) la tenuta dei registri di cui ai successivi artt. 7 e 8;

g) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

4. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

a) il RPD è invitato a partecipare alle riunioni di coordinamento dei soggetti apicali preposti alle singole strutture (Dirigenti e/o P.O.) che abbiano per oggetto questioni inerenti la protezione dei dati personali;

b) il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

c) il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante; nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;

d) il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

5. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti.

In particolare è assicurato al RPD:

a) il supporto attivo per lo svolgimento dei compiti da parte dei soggetti apicali preposti alle singole strutture (Dirigenti e/o P.O.) e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di PEG e di Pianto della performance;

b) tempo sufficiente per l'espletamento dei compiti affidati al RPD;

c) supporto adeguato in termini di risorse finanziare, infrastrutture (sede, attrezzature, strumentazione) e referenti con cui relazionarsi;

d) comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;

e) accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

6. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

In tal senso il RPD:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

7. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento.
In particolare risultano con la stessa incompatibili:
a) il Responsabile per la prevenzione della corruzione e per la trasparenza;
b) il Responsabile del trattamento;
c) qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
8. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti.
In particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.
Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare o ai Responsabili del trattamento.
Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed ai Responsabili del trattamento.

Art. 6

Sicurezza del trattamento

1. Il Comune di Montevarchi e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono:
a) la pseudonimizzazione;
b) la minimizzazione;
c) la cifratura dei dati personali;
d) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
e) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
f) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:

a) sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);

b) misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. Il Comune di Montevarchi e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente presente.

Art.7

Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca le seguenti informazioni:

a) il nome ed i dati di contatto del Comune, del Sindaco ai sensi dell'art.2 del presente regolamento, eventualmente del contitolare del trattamento , del RPD;

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le 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 o organizzazioni internazionali;

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale, compresa l'identificazione del paese terzi o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'art. 49 RGPD, la documentazione delle garanzie adeguate;

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

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate di cui all'art. 6 del presente Regolamento.

2. Il Registro è tenuto dal Titolare ai sensi del precedente art. 2, presso gli uffici della struttura organizzativa del Comune in forma scritta, in formato elettronico, secondo l'allegato A del presente Regolamento.

3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

Art.8

Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile di cui all'art. 4 del presente Regolamento, reca le seguenti informazioni:

a) il nome ed i dati di contatto del Responsabile del trattamento e del RPD;

b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;

c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate di cui all'art. 6 del presente Regolamento.

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma scritta, in formato elettronico, secondo l'allegato B del presente Regolamento.

3. Il Responsabile del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo responsabile.

Art.9

Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35 RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35 RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori; h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative; i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto. Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa.

Il titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno od esterno al Comune.

Il Titolare deve consultarsi con il RPD anche al fine di decidere se effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

Il Responsabile dell'ufficio informatico fornisce supporto al Titolare per lo svolgimento della DPIA.

5. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Il responsabile dell'ufficio informatico può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti: se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP; se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento; ü se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche; se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta. Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;

-dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;
c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati; d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

10. La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento. (eventuale)

11. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 10
Violazione dei dati personali

1. Per violazione dei dati personali (in seguito “data breach”) si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso non autorizzata o l’accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.

2. Il Titolare, in caso di violazione dei dati personali, notifica la violazione all’autorità di controllo competente ai sensi dell’art. 55 RGPD senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che ritenga improbabile che dalla violazione dei dati personali possa derivare un rischio per i diritti e le libertà degli interessati.

Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d’identità; - perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati “elevati” quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un’elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Art.11

Rinvio

1.Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

Allegati

A) schema di registro attività di trattamento
B) schema di registro categorie di attività di trattamento

Allegato A)

Registro attività di trattamento

Comune di Montevarchi

ID	Nome trattamento	Data ultima rilevazione	Struttura competente	Società Titolare	Società Responsabile	DPIA

NOME TRATTAMENTO	
ID TRATTAMENTO	

A. DATI DI CONTATTO

Titolare		Rappresentante del Titolare		Contitolari		Responsabile Protezione Dati	
Struttura	**Contatti**	**Struttura**	**Contatti**	**Struttura**	**Contatti**	**Struttura**	**Contatti**

B. FINALITÀ DEL TRATTAMENTO

Informativa		Tipologia di consenso		Notifica
Rif.	**Descrizione**	**Ref.**	**Descrizione**	**n°**

C. CATEGORIE DI INTERESSATI E DI DATI TRATTATI

Categorie di Interessati del Trattamento

- ☐ Candidati
- ☐ Degenti CRP
- ☐ Clienti
- ☐ Minori
- ☐ Fornitori
- ☐ Familiari
- ☐ Visitatori
- ☐ Collaboratori
- ☐ Soggetti terzi
- ☐ Dipendenti
- ☐ Pazienti SSN
- ☐ Altro, specificare: _____

Natura del dato trattato

- ☐ Personale comune
- ☐ Sensibile
- ☐ Giudiziario

Categoria del dato trattato e soggetti interessati dal trattamento

Categoria del dato	Pazienti	Prospect	Dipendenti	Collaboratori	Candidati	Familiari	Fornitori	Soggetti terzi
☐ Dati identificativi (compresi codici e matricole)	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati comportamentali	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati sensibili	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati genetici	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati giudiziari	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati relativi alla gestione del rapporto di lavoro	☐	☐	☐	☐	☐	☐	☐	☐
☐ Cookies	☐	☐	☐	☐	☐	☐	☐	☐
☐ posizione di veicoli e attrezzature	☐	☐	☐	☐	☐	☐	☐	☐
☐ posizione di persone	☐	☐	☐	☐	☐	☐	☐	☐
☐ Log di sistema (Utenti e AdS)	☐	☐	☐	☐	☐	☐	☐	☐

D. CATEGORIE DI DESTINATARI UE e EXTRA UE

Nome	Finalità del trasferimento	Tipologia di destinatario	UE	Extra UE	Garanzie adeguate in caso di destinatari extra UE)					
					Consenso	Privacy Shield (USA)	BCR	Data Protection Agreement	Model contract clauses	Certificazioni
		☐ Titolari ☐ Resp. esterni ☐ Org. internaz.	☐	☐	☐	☐	☐	☐	☐	☐
		☐ Titolari ☐ Resp. esterni ☐ Org. internaz.	☐	☐	☐	☐	☐	☐	☐	☐

E. CONSERVAZIONE E CANCELLAZIONE DEI DATI

Categoria del dato trattato	Periodo di conservazione	Action al termine del periodo di retention	
		Anonimizzazione	Cancellazione
☐ Dati identificativi (compresi codici e matricole)		☐	☐
☐ Dati comportamentali		☐	☐
☐ Dati sensibili		☐	☐
☐ Dati genetici		☐	☐
☐ Dati giudiziari		☐	☐
☐ Dati relativi alla gestione del rapporto di lavoro		☐	☐
☐ Cookies		☐	☐
☐ posizione di veicoli e attrezzature		☐	☐
☐ posizione di persone		☐	☐
☐ Log di sistema (Utenti e AdS)		☐	☐

F. STRUMENTI UTILIZZATI PER IL TRATTAMENTO

ID	Nome	Descrizione e utilizzo	Note

G.1 MISURE DI SICUREZZA ORGANIZZATIVE

Distribuzione dei Ruoli e Responsabilità	**Formazione**	**Policy, Procedure, Istruzioni operative**
Meccanismi incentivanti per i soggetti coinvolti	**Misure per Privacy by Design / Privacy by Default**	**Clausole contrattuali / SLA con le terze parti interessate**
Misure prescrittive organizzative per amministratori di sistema	**Misure prescrittive organizzative per l'utilizzo delle risorse informatiche**	**Misure prescrittive organizzative per videosorveglianza**
Misure prescrittive organizzative per FSE/CE	**Misure prescrittive organizzative per i trial clinici**	**Misure prescrittive organizzative per la refertazione on-line**
Misure prescrittive organizzative per dati genetici	**Misure prescrittive organizzative per marketing su dati sanitari**	**Monitoraggio periodico delle misure organizzative e operative**
Crittografia	**Audit Interno periodico - monitoraggio**	**Adesione a Codice di Condotta (art.40 GDPR)**
Adesione meccanismo di certificazione (art. 42 GDPR)		

G.2 MISURE DI SICUREZZA TECNOLOGICHE

G.3 MISURE DI SICUREZZA FISICHE

H. VALUTAZIONE DPIA

1 Trattamenti valutativi o di scoring	2 Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura	3 Monitoraggio sistematico	4 Dati sensibili o dati di natura estremamente personale	5 Trattamenti di dati su larga scala	6 Combinazione o raffronto di insiemi di dati	7 Dati relativi a interessati vulnerabili	8 Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative	9 Trattamenti che "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto

Ci sono eccezioni per le quali la DPIA non risulta essere obbligatoria?	Valutazione della necessità e proporzionalità del trattamento in relazione alle finalità;	Sono stati coinvolti soggetti interessati per la valutazione dei rischi Privacy?	Fa parte dell'elenco delle tipologie di trattamenti per le quali l'Autorità di controllo ha pubblicato che non è richiesta una valutazione d'impatto sulla protezione dei dati?

I. PROFILO DI RISCHIO

Profilo di rischio preliminare	**Inserire data**	**Valutazione preliminare Autorità Garante (solo per trattamenti con profilo di rischio residuo Alto dopo DPIA)**	**Inserire data**
	Inserire livello di rischio (Non Alto/Alto)		Esiti della consultazione preventiva
Profilo di rischio post Data Protection Impact Assessment	**Inserire data**		Link al provvedimento
	Inserire livello di rischio (Non Alto/Alto)		

Allegato B)

Registro categorie di attività di trattamento						
Comune di Montevarchi						
ID	**Nome trattamento**	**Data ultima rilevazione**	**Struttura competente**	**Società Titolare**	**Società Responsabile**	**DPIA**

NOME TRATTAMENTO	
ID TRATTAMENTO	

A. DATI DI CONTATTO

Responsabile		Titolare		Rappresentante del Titolare		Contitolari		Responsabile Protezione	
Struttura	Contatti	Struttura	Contatti	Struttura	Contatti	Struttura	Contatti	Struttura	Contatti

B. FINALITÀ DEL TRATTAMENTO

Informativa		Tipologia di consenso		Notifica n.
Rif.	Descrizione	Ref.	Descrizione	

C. CATEGORIE DI INTERESSATI E DI DATI TRATTATI

Categorie di Interessati del Trattamento

- ☐ Candidati
- ☐ Degenti CRP
- ☐ Clienti
- ☐ Minori
- ☐ Fornitori
- ☐ Familiari
- ☐ Visitatori
- ☐ Collaboratori
- ☐ Soggetti terzi
- ☐ Dipendenti
- ☐ Pazienti SSN
- ☐ Altro, specificare_____

Natura del dato trattato

- ☐ Personale comune
- ☐ Sensibile
- ☐ Giudiziario

Categoria del dato trattato e soggetti interessati dal trattamento

Categoria del dato	Pazienti	Prospect	Dipendenti	Collaboratori	Candidati	Familiari	Fornitori	Soggetti terzi
☐ Dati identificativi (compresi codici e matricole)	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati comportamentali	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati sensibili	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati genetici	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati giudiziari	☐	☐	☐	☐	☐	☐	☐	☐
☐ Dati relativi alla gestione del rapporto di lavoro	☐	☐	☐	☐	☐	☐	☐	☐
☐ Cookies	☐	☐	☐	☐	☐	☐	☐	☐
☐ posizione di veicoli e attrezzature	☐	☐	☐	☐	☐	☐	☐	☐
☐ posizione di persone	☐	☐	☐	☐	☐	☐	☐	☐
☐ Log di sistema (Utenti e AdS)	☐	☐	☐	☐	☐	☐	☐	☐

D. CATEGORIE DI DESTINATARI UE e EXTRA UE

Nome	Finalità del trasferimento	Tipologia di destinatario	UE	Extra UE	Garanzie adeguate in caso di destinatari extra UE)					
					Consenso	Privacy Shield (USA)	BCR	Data Protection Agreement	Model contract clauses	Certificazioni
		☐ Titolari	☐	☐	☐	☐	☐	☐	☐	☐
		☐ Resp. esterni								
		☐ Org. internaz.								
		☐ Titolari	☐	☐	☐	☐	☐	☐	☐	☐
		☐ Resp. esterni								
		☐ Org. internaz.								

E. CONSERVAZIONE E CANCELLAZIONE DEI DATI

Categoria del dato trattato	Periodo di conservazione	Action al termine del periodo di retention	
		Anonimizzazione	Cancellazione
☐ Dati identificativi (compresi codici e matricole)		☐	☐
☐ Dati comportamentali		☐	☐
☐ Dati sensibili		☐	☐
☐ Dati genetici		☐	☐
☐ Dati giudiziari		☐	☐
☐ Dati relativi alla gestione del rapporto di lavoro		☐	☐
☐ Cookies		☐	☐
☐ posizione di veicoli e attrezzature		☐	☐
☐ posizione di persone		☐	☐
☐ Log di sistema (Utenti e AdS)		☐	☐

F. STRUMENTI UTILIZZATI PER IL TRATTAMENTO

ID	Nome	Descrizione e utilizzo	Note

G.1 MISURE DI SICUREZZA ORGANIZZATIVE

Distribuzione dei Ruoli e Responsabilità	Formazione	Policy, Procedure, Istruzioni operative
Meccanismi incentivanti per i soggetti coinvolti	Misure per Privacy by Design / Privacy by Default	Clausole contrattuali / SLA con le terze parti interessate
Misure prescrittive organizzative per amministratori di sistema	Misure prescrittive organizzative per l'utilizzo delle risorse informatiche	Misure prescrittive organizzative per videosorveglianza
Misure prescrittive organizzative per FSE/CE	Misure prescrittive organizzative per i trial clinici	Misure prescrittive organizzative per la refertazione on-line
Misure prescrittive organizzative per dati genetici	Misure prescrittive organizzative per marketing su dati sanitari	Monitoraggio periodico delle misure organizzative e operative
Crittografia	Audit Interno periodico - monitoraggio	Adesione a Codice di Condotta (art.40 GDPR)
Adesione meccanismo di certificazione (art. 42 GDPR)		

G.2 MISURE DI SICUREZZA TECNOLOGICHE

G.3 MISURE DI SICUREZZA FISICHE

H. VALUTAZIONE DPIA

1	2	3	4	5	6	7	8	9
Trattamenti valutativi o di scoring	Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura	Monitoraggio sistematico	Dati sensibili o dati di natura estremamente personale	Trattamenti di dati su larga scala	Combinazione o raffronto di insiemi di dati	Dati relativi a interessati vulnerabili	Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative	Trattamenti che "impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto

Ci sono eccezioni per le quali la DPIA non risulta essere obbligatoria?	Valutazione della necessità e proporzionalità del trattamento in relazione alle finalità;	Sono stati coinvolti soggetti interessati per la valutazione dei rischi Privacy?	Fa parte dell'elenco delle tipologie di trattamenti per le quali l'Autorità di controllo ha pubblicato che non è richiesta una valutazione d'impatto sulla protezione dei dati?

I. PROFILO DI RISCHIO

Profilo di rischio preliminare	**Inserire data**	**Valutazione preliminare Autorità Garante (solo per trattamenti con profilo di rischio residuo Alto dopo DPIA)**	**Inserire data**
	Inserire livello di rischio (Non Alto/Alto)		Esiti della consultazione preventiva
Profilo di rischio post Data Protection Impact Assessment	**Inserire data**		Link al provvedimento
	Inserire livello di rischio (Non Alto/Alto)		

* Le misure di sicurezza tecniche sono associate ai singoli strumenti di trattamento, nelle relative schede (e.g. Pseudonimizzazione e cifratura dei dati)