Modello organizzativo del Comune di Carpi in materia di protezione dei dati personali

Sommario

Art. 1 – Oggetto

Il presente modello organizzativo ha per oggetto misure procedimentali e regole di dettaglio finalizzate a garantire la migliore funzionalità ed efficacia nell'attuazione, all'interno del Comune di Carpi, delle disposizioni di cui al 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 Protezione Dati, di seguito anche "GDPR"), nonché della normativa interna di adeguamento al predetto Regolamento di cui al D. Lgs. del 10 agosto 2018, n. 101, che ha novellato il D. Lgs. 196/2003 (di seguito anche "Codice Privacy").

Con il presente modello organizzativo, il Comune di Carpi individua le politiche, gli obiettivi e gli standard di sicurezza finalizzati a garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro complessivo delle misure di sicurezza informatiche, logiche, fisiche, organizzative e procedurali da adottare e da applicare per attenuare e, ove possibile, eliminare il rischio di violazione dei dati derivante dal trattamento.

Art. 2 – Definizioni

Al fine di garantire una migliore comprensione del presente modello organizzativo, risulta opportuno dettagliare le seguenti definizioni:

- **Amministratori di sistema**: le figure professionali espressamente designate dal Dirigente competente per il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine per la gestione e la manutenzione di un sistema informativo o di sue componenti (provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recante *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*, pubblicato sulla G.U. del 24 dicembre 2008, così come modificato dal successivo provvedimento del 25 Giugno 2009);
- **Autorità di controllo**: l'Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del GDPR;
- **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;
- **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 di categorie particolari**: i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi a identificare in modo unico una persona fisica, dati relativa alla salute o alla vista sessuale o all'orientamento sessuale della persona, dati attinenti alla salute fisica o mentale di una persona (compresa la prestazione di servizi di assistenza sanitaria), che rilevano informazioni relative al suo stato di salute;
- **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 personali**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (c.d. "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;
- **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 rivelino informazioni relative al suo stato di salute;

- ***Privacy by default***: il principio del GDPR secondo cui il Titolare del trattamento deve mettere in atto misure tecniche ed organizzative idonee a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari al perseguimento di ogni specifica finalità per cui sono stati raccolti. Tale obbligo si applica alla quantità di dati personali raccolti, all'estensione del loro trattamento, al periodo di conservazione e all'accessibilità degli stessi. In particolare, tali misure garantiscono che per impostazione predefinita i dati personali non siano accessibili ad un numero indefinito di persone fisiche senza l'intervento del singolo;
- ***Privacy by design***: il principio del GDPR secondo cui, tenuto conto dello stato dell'arte e dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, il Titolare del trattamento deve mettere in atto, sia al momento della determinazione dei mezzi di trattamento sia all'atto del trattamento stesso, misure tecniche ed organizzative, quali la pseudonimizzazione, progettate per attuare in modo efficace i principi concernenti la protezione dei dati, come la minimizzazione dei dati, per integrare nel trattamento le garanzie necessarie a soddisfare i requisiti posti dal GDPR e per tutelare i diritti degli interessati;
- **Profilazione**: qualsiasi forma di trattamento automatizzato di 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;
- **Responsabile della protezione dei dati personali**: figura nominata dal Titolare del trattamento nei casi previsti dall'art. 37 del GDPR, che ricopre la posizione prevista dall'art 38 e svolge i compiti previsti dall'art. 39 del medesimo GDPR;
- **Responsabile del trattamento (esterno)**: la persona fisica, la persona giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- **Soggetti autorizzati al trattamento dei dati personali**: i soggetti designati e le persone autorizzate a compiere operazioni di trattamento dei dati personali (incaricati) e che operano sotto l'autorità diretta del Titolare e dei soggetti designati;
- **Soggetti designati a specifici compiti e funzioni**: i soggetti attuatori degli adempimenti previsti dalla normativa vigente in materia di trattamento dei dati personali, ai quali il Titolare del trattamento conferisce, mediante atti di designazione espressa, specifici compiti e funzioni connessi al trattamento di dati relativamente ai Settori/Servizi di rispettiva competenza, fornendo le relative istruzioni utili ai fini della corretta attuazione dei compiti e delle funzioni loro conferite;
- **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;
- **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;
- **Trattamento dei dati personali relative a condanne penali e reati**: i dati personali relativi a condanne penali e reati;
- **Trattamento transfrontaliero**: il 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, ovvero il 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 presenti in più di uno Stato membro;
- **Violazione dei dati personali (*data breach*)**: 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.

Art. 3 – Trattamento dei dati personali

Il trattamento dei dati personali è compiuto dal Comune di Carpi per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
b) l'adempimento di un obbligo legale al quale è soggetto il Comune di Carpi;
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.

Il Comune di Carpi tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali, così come previste da disposizioni di legge, statutarie e regolamentari, in conformità e nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti emanati dall'Autorità di controllo.
Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti appositamente designati e autorizzati. Non è consentito il trattamento da parte di persone non autorizzate ed istruite in tal senso.

Nell'ambito delle operazioni di trattamento il Comune di Carpi tratta totalmente o parzialmente, anche in modo automatizzato, le seguenti tipologie di dati:

- dati personali, così come definiti dall'articolo 4, paragrafo 1, del GDPR;
- categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del GDPR e all'articolo 2-*septies* del Codice Privacy;
- dati personali relativi a condanne penali e reati (c.d. dati giudiziari) di cui all'articolo 10 del GDPR e all'articolo 2-*octies* del Codice Privacy.

Art. 4 – Titolare del trattamento

Ai sensi dell'art. 4, paragrafo 7, del GDPR, il Comune di Carpi è il Titolare del trattamento (di seguito anche solo "Titolare") dei dati personali raccolti o meno in banche dati, automatizzate o cartacee.
Il Titolare è responsabile del rispetto dei principi applicabili al trattamento dei dati personali stabiliti dall'art. 5 del GDPR: liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

Altresì il Titolare, ai sensi dell'art. 24 del GDPR, mette in atto misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento di dati personali sia effettuato in modo conforme alla normativa vigente in materia di protezione dei dati personali.
Le misure sono definite sin dalla fase della progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati nonché agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15 e seguenti del GDPR, unitamente alle comunicazioni e alle informazioni occorrenti per il loro esercizio.
Gli interventi necessari per l'attuazione delle suddette misure sono considerati nell'ambito della programmazione operativa (DUP), del bilancio e del 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.

Il Titolare, inoltre:

a) adotta, nelle forme previste dal proprio ordinamento, gli interventi normativi e organizzativi necessari per assicurare la conformità dei trattamenti alle disposizioni previste dalla normativa vigente in materia di protezione dei dati personali;
b) provvede, ai sensi dell'art. 37 del GDPR, a designare il Responsabile della Protezione dei Dati (di seguito anche "RPD") ponendolo in grado di svolgere adeguatamente le attività e i compiti previsti dagli artt. 38 e 39 del GDPR;
c) tenuto conto dell'assetto organizzativo-direzionale dell'Ente, attribuisce specifici compiti e funzioni ai soggetti designati per l'attuazione degli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali. A tal fine il Titolare provvede attraverso l'adozione di atti di designazione espressa, fornendo le relative istruzioni utili ai fini della corretta attuazione dei compiti e delle funzioni loro conferite;

d) istruisce i soggetti autorizzati al trattamento dei dati personali;
e) istituisce, ai sensi dell'art. 30 del GDPR, i Registri delle attività di trattamento svolte sotto la propria responsabilità e verifica che gli stessi siano periodicamente aggiornati;
f) provvede a garantire adeguata pubblicità circa l'assetto organizzativo adottato dall'Ente in materia di protezione dei dati personali, pubblicando l'elenco delle persone fisiche espressamente designate sulla base di quanto previsto al precedente punto c) sul sito internet dell'Ente nonché nella rete intranet;

Art. 5 – Soggetti designati a specifici compiti e funzioni

Tenuto conto dei principi sull'Ordinamento degli Enti locali e dell'attuale assetto organizzativo-direzionale dell'Ente, sono designati quali soggetti attuatori degli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali (di seguito anche solo "soggetti designati") i Dirigenti di ciascun Settore in cui si articola la struttura organizzativa dell'Ente. A tali soggetti il Titolare, mediante l'adozione di atti di designazione espressa, attribuisce specifici compiti e funzioni connessi al trattamento dei dati personali inerenti al Settore di rispettiva competenza, fornendo le relative istruzioni utili ai fini della corretta attuazione dei compiti e delle funzioni loro conferite.

I Dirigenti di ciascun Settore, quali soggetti designati a cui sono attribuiti specifici compiti e funzioni per l'attuazione degli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali, sono in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, necessarie per mettere in atto misure tecniche e organizzative volte a garantire che i trattamenti siano effettuati in conformità alla normativa vigente in materia di protezione dei dati personali.

Relativamente ai trattamenti di dati personali trasversali a più Settori/Servizi, ciascun Settore è responsabile dei rispettivi trattamenti.

Nell'ambito del Settore di rispettiva competenza, ciascun soggetto designato provvede a:
a) verificare la legittimità dei trattamenti di dati personali effettuati;
b) disporre eventualmente, a seguito delle verifiche di cui alla precedente lett. a), le modifiche necessarie al trattamento affinché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione della stessa;
c) adottare soluzioni di *privacy by design* e *by default*, predisponendo sin dall'inizio adeguate ed indispensabili misure tecniche ed organizzative che, tenuto conto dello state dell'arte, dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità dei trattamenti, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, garantiscano la conformità degli stessi alla normativa vigente in materia;
d) effettuare, in collaborazione con il RPD ed eventualmente con il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine, l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli interessati;
e) svolgere, in collaborazione con il RPD ed eventualmente con il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine, la preventiva valutazione d'impatto ai sensi dell'art. 35 del GDPR, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità dello stesso, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
f) verificare ed adottare, in collaborazione con il RPD ed eventualmente con il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine, idonee misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti effettuati;
g) effettuare periodicamente la ricognizione integrale dei trattamenti svolti, aggiornando i relativi Registri del trattamento;
h) predisporre le informative relative al trattamento dei dati personali nel rispetto degli artt. 13 e 14 del GDPR;
i) garantire, in collaborazione con il RPD, la corretta informazione e l'esercizio dei diritti degli interessati, provvedendo a dare riscontro alle istanze degli stessi;

j) identificare e a designare per iscritto i soggetti autorizzati a compiere operazioni di trattamento, fornendo agli stessi le istruzioni per il corretto trattamento dei dati, nel rispetto delle istruzioni impartite dal Titolare;
k) controllare costantemente che le persone fisiche autorizzate al trattamento dei dati effettuino le operazioni di trattamento in attuazione delle istruzioni ricevute, nonché in conformità alle istruzioni fornite dal Titolare e nel rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza;
l) designare i referenti privacy che faranno parte del Gruppo referenti privacy di cui al successivo art. 16;
m) sensibilizzare, formare ed istruire il personale che partecipa ai trattamenti ed alle connesse attività di controllo;
n) designare, ai sensi dell'art. 28 del GDPR, i Responsabili del trattamento, avendo cura di tenere costantemente aggiornati i Registri nonché la relativa documentazione;
o) garantire al RPD ed agli Amministratori di sistema del Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di eventuali incidenti di sicurezza;
p) collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
q) attivare la procedura per la gestione della violazione dei dati personali (c.d. "data breach"), informando tempestivamente, senza ingiustificato ritardo, il RPD e procedere, in collaborazione con lo stesso ed eventualmente con il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine, all'analisi e alla valutazione della gravità della violazione, anche ai fini della successiva eventuale notifica all'Autorità di controllo e comunicazione agli interessati ai sensi degli artt. 33 e 34 del GDPR;
r) disporre, in collaborazione con il RPD ed eventualmente con il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine, l'adozione dei provvedimenti imposti dall'Autorità di controllo;

Oltre alle attività sopra citate, ciascun soggetto designato provvede, relativamente al Settore di rispettiva competenza, a tutte le attività previste dalla legge e a tutti gli specifici compiti e funzioni conferiti dal Titolare, analiticamente specificati per iscritto nell'atto di designazione.

Fermo restando che le responsabilità delle attività sopra citate rimane, in ogni caso, in capo ai soggetti designati relativamente ai Settori/Servizi di rispettiva competenza, in ragione del fatto che non sono ascrivibili a funzioni di direzione, coordinamento generale e controllo, in base ai principi generali relativi all'istituto della delega, sono eventualmente sub-delegabili i compiti di cui alle lettere g), h), i), p).
Tali compiti sono sub-delegabili ai Responsabili P.O. ovvero, in mancanza, a funzionari presenti nei Settori/Servizi diretti dai soggetti designati.

Nell'esecuzione degli specifici compiti e funzioni conferiti per l'attuazione degli adempimenti previsti dalla normativa vigente in materia di protezione dei dati personali relativamente al Settore di rispettiva competenza, ciascun soggetto designato garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione in materia di trattamento dei dati personali e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

Art. 6 – Responsabile della Protezione dei Dati (RPD)

Il Responsabile della Protezione dei Dati (RPD) è designato dal Titolare con apposito atto ai sensi degli artt. 37-39 del GDPR.
Il RPD, nel rispetto di quanto previsto dall'art. 39 del GDPR, è incaricato di svolgere, in piena autonomia e indipendenza, i seguenti compiti e funzioni:

- 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 dal GDPR, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione europea relative alla protezione dei dati, nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresa l'attribuzione delle responsabilità,

la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del GDPR;
- cooperare con l'Autorità di controllo;
- fungere da punto di contatto con l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

I compiti del RPD attengono all'insieme dei trattamenti di dati effettuati dal Comune di Carpi.

In merito alle attività e ai compiti propri del RPD, il Comune di Carpi si impegna a:
- mettere a disposizione del RPD le risorse necessarie al fine di consentire a quest'ultimo l'ottimale svolgimento dei compiti e delle funzioni assegnate;
- non rimuovere o penalizzare il RPD in ragione dell'adempimento dei compiti affidati nell'esercizio delle sue funzioni;
- garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto di interesse

I dati di contatto del RPD sono pubblicati sul sito web istituzionale del Comune di Carpi, rendendoli accessibili da un apposito link, comunicati all'Autorità di controllo, ai componenti della Giunta del Comune di Carpi, a tutto il personale dipendente del Comune di Carpi, nonché inclusi in tutte le informative rese agli interessati ai sensi degli artt. 13 e 14 del GDPR.

Art. 7 – Soggetti autorizzati al trattamento dei dati personali

Sono autorizzati a compiere operazioni di trattamento dei dati personali i soggetti designati di cui all'art. 5 del presente modello organizzativo e i loro delegati.
I soggetti designati e i loro delegati conformano i trattamenti relativi al Settore di rispettiva competenza alle istruzioni fornite dal Titolare, nonché alle istruzioni di seguito riportate:
- le operazioni di trattamento devono essere effettuate in attuazione dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza;
- sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- sono verificati legittimità e correttezza dei trattamenti e, in particolar modo, i rischi che gli stessi presentano nonché la natura dei dati personali da proteggere.

Altresì, sono autorizzati tutti i soggetti (di seguito anche solo "incaricati") che effettuano operazioni di trattamento, dipendenti e collaboratori che, a qualsiasi titolo, operano sotto la diretta autorità del Titolare o dei soggetti designati.
Gli incaricati sono designati per iscritto tramite individuazione nominativa delle persone fisiche autorizzate a compiere operazioni di trattamento con l'indicazione, per ciascun nominativo, dei trattamenti che il soggetto è autorizzato ad effettuare.
Inoltre, la designazione deve contenere le istruzioni impartite agli incaricati, anche riguardanti eventuali aspetti di dettaglio da diversificare in ragione della specificità dei singoli trattamenti e devono contenere un espresso richiamo alle istruzioni fornite dal Titolare.
In ogni caso, l'autorizzazione conferita dal Titolare e/o dai soggetti dallo stesso designati decade a seguito di dimissioni e/o cessazione dei compiti che giustificano il trattamento dei dati personali. In caso di destinazione a differenti mansioni si potrà procedere alla modifica/aggiornamento dell'autorizzazione conferita.

Art. 8 – Compiti e funzioni del Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine

L'Unione delle Terre d'Argine ed i Comuni ad essa aderenti, a seguito di apposita Convenzione approvata con Deliberazione del Consiglio dell'Unione n. 29 del 22/12/2010, hanno trasferito all'Unione delle Terre d'Argine le competenze inerenti alla gestione dei Sistemi Informativi e del Servizio Informativo – Statistico.

Al Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine e al soggetto designato competente per tale Settore spetta il compito di:

- elaborare, in collaborazione con il Settore Risorse Umane dell'Unione delle Terre d'Argine, norme di comportamento relative alla sicurezza informatica e alla protezione dei dati personali finalizzate a garantire, all'interno dell'Unione delle Terre d'Argine e dei Comuni ad essa aderenti, il rispetto della normativa vigente in materia di protezione dei dati personali nell'utilizzo degli strumenti elettronici e cartacei degli Enti, da aggiornare periodicamente ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;
- nel caso in cui si proceda alla stipula di contratti finalizzati allo sviluppo e all'acquisizione di software e piattaforme, elaborare policy adeguate a garantire la sicurezza informatica e la protezione dei dati personali relativamente allo sviluppo delle applicazioni informatiche, da richiamare nei predetti contratti, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del contratto;
- individuare misure adeguate ed efficaci per garantire la tutela dell'integrità, della riservatezza e disponibilità del patrimonio informativo dell'Unione delle Terre d'Argine e dei Comuni ad essa aderenti, condividendole preventivamente con il RPD;
- provvedere, nel caso in cui venga avvertito un problema di sicurezza informatica, a:
  a) collaborare con il RPD e i soggetti designati rispettivamente competenti in caso di violazione dei dati personali;
  b) individuare le misure ritenute idonee a garantire il miglioramento della sicurezza informatica dei trattamenti di dati personali, in collaborazione con il RPD;
- svolgere opportune verifiche in merito all'osservanza della normativa in materia di sicurezza delle informazioni e del trattamento dei dati personali, in collaborazione con il RPD e i soggetti designati di ciascun Settore;
- svolgere in collaborazione con il RPD e i soggetti designati rispettivamente competenti, la preventiva valutazione d'impatto ai sensi dell'art. 35 del GDPR, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- promuovere, in collaborazione con il Settore Risorse Umane dell'Unione delle Terre d'Argine e il RPD, la formazione del personale dell'Unione delle Terre d'Argine e dei Comuni ad essa aderenti in materia di sicurezza informatica.

Inoltre, al soggetto designato competente per il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine spetta il compito di designare gli Amministratori di sistema, coerentemente a quanto previsto dalla normativa vigente in materia.

Art. 9 – Amministratori di sistema del Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine

Tenuto conto di quanto previsto dal Garante per la protezione dei dati personali con provvedimento del 27/11/2008, recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", così come modificato con successivo provvedimento del 25/06/2009, l'Unione delle Terre d'Argine ed i Comuni ad essa aderenti si avvalgono delle professionalità operanti all'interno del Settore Sistemi Informativi Associati che, in qualità di Amministratori di sistema, garantiscono che i sistemi informativi dell'Unione delle Terre d'Argine e dei Comuni ad essa aderenti siano strutturati e gestiti in modo tale da consentire l'attuazione delle misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso i predetti sistemi.

L'Amministratore di sistema, così come individuato ed espressamente designato per iscritto dal Dirigente competente per il suddetto Settore previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.
Nell'atto di designazione devono essere dettagliati i compiti spettanti all'Amministratore di sistema così come previsti dalla normativa vigente in materia.
In particolare, spetta all'Amministratore di sistema la cura dei seguenti adempimenti:

a) la gestione hardware e software dei server e delle postazioni di lavoro informatizzate;
b) l'impostazione e la gestione di un sistema di autenticazione e autorizzazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
c) la registrazione degli accessi logici (autenticazione e autorizzazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte degli Amministratori di sistema;
d) l'impostazione e la gestione di un sistema di autorizzazione per tutti coloro che siano autorizzati all'accesso ai dati personali contenuti nelle banche dati informatizzate;
e) la verifica costante circa l'efficacia delle misure tecniche e organizzative adottate per garantire la sicurezza informatica dei dati personali dell'Unione delle Terre d'Argine e dei Comuni ad essa aderenti, provvedendo senza indugio agli adeguamenti eventualmente necessari per la loro correzione e/o implementazione;
f) l'aggiornamento, almeno con cadenza annuale, della relazione relativa all'efficacia delle misure tecniche ed organizzative adottate per garantire la sicurezza informatica dei dati personali, da inviare all'Unione delle Terre d'Argine e dei Comuni ad essa aderenti in qualità di Titolari. Tale relazione deve includere anche eventuali segnalazioni e suggerimenti relativi all'adozione di ulteriori misure tecniche ed organizzative e/o all'aggiornamento di quelle esistenti in ragione delle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche dei trattamenti. Tanto, al fine di consentire ai Titolari del trattamento la programmazione degli adempimenti amministrativi e contabili finalizzati all'adozione di quanto segnalato e/o suggerito dagli Amministratori di sistema.

Oltre agli adempimenti sopra citati, l'Amministratore di sistema provvede a tutti gli eventuali ulteriori adempimenti analiticamente specificati per iscritto nell'atto di designazione.

Il soggetto designato competente per il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine e il RPD procederanno periodicamente alla verifica delle attività svolte dagli Amministratori dei sistemi informatici designati al fine di controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza previste dalla vigente normativa in riferimento ai trattamenti dei dati personali.

Art. 10 – Contitolare del trattamento

Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune di Carpi da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento (contitolarità), l'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in materia di protezione dei dati personali, con particolare riferimento all'esercizio dei diritti degli interessati e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dal diritto nazionale.
L'accordo più individuare un punto di contatto comune per gli interessati.

Art. 11 – Responsabile del trattamento

Tenuto conto di quanto previsto dall'art. 28 del GDPR, nel caso in cui soggetti esterni all'Ente siano tenuti, ad esempio a seguito di convenzione, contratto, verbale di aggiudicazione, provvedimento di nomina, ad effettuare trattamenti di dati personali per conto dell'Ente, gli stessi devono essere designati quali Responsabili del trattamento. I Responsabili del trattamento devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalla normativa vigente in materia di trattamento dei dati personali e garantisca la tutela dei diritti degli interessati.

I soggetti designati, tenuto conto di quanto previsto dall'art. 28, paragrafi 3 e 9, del GDPR, identificano i Responsabili del trattamento relativamente ai trattamenti effettuati nel Settore di rispettiva competenza e stipulano con questi ultimi, in forma scritta o in formato elettronico, i relativi contratti e/o altri atti giuridici a norma del diritto nazionale ed europeo per il trattamento dei dati.
Tali contratti e/o altri atti giuridici devono vincolare il Responsabile del trattamento al Titolare del trattamento, stipulare la materia disciplinata, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie degli interessati, nonché gli obblighi e i diritti del Titolare del trattamento.

La liceità dell'attività di trattamento dei dati da parte del Responsabile del trattamento è determinata dal mandato ricevuto dal Titolare del trattamento. Se va al di là del proprio mandato, acquisendo un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il Responsabile del trattamento diventa Titolare del trattamento.
Ai fini della corretta qualificazione del ruolo soggettivo rivestito dal ciascuna delle parti (Titolare o Responsabile del trattamento) all'interno di qualsivoglia rapporto intercorrente tra il Comune di Carpi e un altro soggetto, pubblico o privato, l'Ente adotta il criterio della valutazione delle circostanze di fatto.

Inoltre, ciascun soggetto designato, relativamente al Settore di rispettiva competenza, provvede all'aggiornamento della documentazione relativa ai predetti contratti/atti giuridici, all'acquisizione dai Responsabili e dagli eventuali Sub-responsabili dell'elenco nominativo delle persone fisiche che, presso gli stessi, risultino autorizzate al trattamento dei dati e a compiere le relative operazioni, nonché alla verifica del rispetto da parte dei Responsabili e degli eventuali Sub-responsabili delle prescrizioni contenute nei contratti/atti giuridici sottoscritti, inclusa la verifica, in collaborazione con gli Amministratori di sistema, circa l'adozione da parte degli stessi di adeguate misure di sicurezza tecniche ed organizzative.
La periodicità delle predette verifiche, prevista nel relativo contratto/atto giuridico, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati sono condivisi dal Responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

Art. 12 Sicurezza del trattamento

Il Titolare, nonché ciascun soggetto designato relativamente al Settore di rispettiva competenza, in collaborazione con il RPD ed eventualmente anche con il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine, provvedono a mettere in atto le misure tecniche ed organizzative necessarie a 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.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono, ad esempio: la pseudonimizzazione, la minimizzazione, la cifratura dei dati personali, la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico, una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

A titolo esemplificativo e non esaustivo, costituiscono misure tecniche ed organizzative che possono essere adottate:

- sistemi di autenticazione, sistemi di autorizzazione, sistemi di protezione (antivirus, firewall, antintrusione, altro);
- 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.

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

Il Titolare, nonché ciascun soggetto designato relativamente al Settore di rispettiva competenza, impartiscono adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

Art. 13 – Registri delle attività di trattamento

Il Registro delle attività di trattamento svolte dal Comune di Carpi in qualità di Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome e i dati di contatto del Comune di Carpi, dell'eventuale Contitolare del trattamento e del Responsabile della Protezione dei Dati;
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;
e) l'eventuale trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come previste dall'art. 32, paragrafo 1, del GDPR.

Il Registro delle attività di trattamento svolte dal Comune di Carpi in qualità di Responsabile del trattamento reca almeno le seguenti informazioni:

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 il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come previste dall'art. 32, paragrafo 1, del GDPR.

I Registri sono tenuti in forma telematica e/o cartacea.
Ciascun soggetto designato ha la responsabilità, relativamente al Settore di rispettiva competenza, di effettuare periodicamente la ricognizione integrale dei trattamenti svolti, aggiornando i relativi Registri del trattamento.

Il RPD svolge una funzione di controllo relativamente alla tenuta e all'aggiornamento dei Registri delle attività di trattamento.

Art. 14 – Valutazioni d'impatto sulla protezione dei dati (DPIA)

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 soggetto designato, prima di effettuare il trattamento ed in collaborazione con il RPD ed eventualmente anche con il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 del GDPR, 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 del trattamento alle norme vigenti in materia di protezione dei dati personali.

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 dall'Autorità di controllo ai sensi dell'art. 35, paragrafi 4-6, del GDPR.

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, paragrafo 3, del GDPR, 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 sulle suddette 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 particolari o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del GDPR;
e) trattamenti di dati su larga scala, tenendo conto del numero dei soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento, del volume dei dati e/o dell'ambito delle diverse tipologie di dati oggetto di trattamento, della durata o persistenza dell'attività di trattamento, dell'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 i soggetti designati ritengano motivatamente che non possa presentare un rischio elevato. I soggetti designati possono motivatamente ritenere che, per un trattamento che soddisfi solo uno dei criteri di cui sopra, occorra comunque la conduzione di una DPIA.

I soggetti designati garantiscono l'effettuazione della DPIA e sono responsabili della stessa. I soggetti designati devono consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA. Tale consultazione e le conseguenti decisioni assunte dai soggetti designati devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

La DPIA non è necessaria nei casi seguenti:

1. se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del GDPR;
2. 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;
3. se il trattamento è stato sottoposto a verifica da parte dell'Autorità di controllo prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
4. 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 dell'Autorità di controllo o del RPD e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni dell'Autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

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

- 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);
- 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;
    - della consultazione preventiva dell'Autorità di controllo;
- 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;
- individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con la normativa vigente in materia di protezione dei dati personali, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

I soggetti designati, relativamente al Settore di rispettiva competenza, possono 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.

Nel caso in cui le risultanze della DPIA indichino l'esistenza di un rischio residuale elevato, i soggetti designati procedono, unitamente al RPD, alla consultazione preventiva dell'Autorità di controllo. I soggetti designati, unitamente al RPD, consultano l'Autorità di controllo 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.

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.

Art. 15 – Violazione dei dati personali

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 autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune di Carpi.

Relativamente al Settore di rispettiva competenza, i soggetti designati attivano la procedura per la gestione della violazione dei dati personali (c.d. "*data breach*"), informando tempestivamente, senza ingiustificato ritardo, il RPD e procedono, in collaborazione con il RPD ed eventualmente con il Settore Sistemi Informativi Associati dell'Unione delle Terre d'Argine, all'analisi e alla valutazione della gravità della violazione stessa. Qualora, a conclusione di tale analisi e valutazione, si ritenga probabile che dalla violazione siano derivati rischi per i diritti e la libertà degli interessati, i soggetti designati rispettivamente

competenti provvedono, entro 72 ore e comunque senza ingiustificato ritardo, alla notifica della violazione all'Autorità di controllo.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando n. 75 del GDPR, 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).

Se i soggetti designati ritengono che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, allora devono informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di far 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).

La notifica all'Autorità di controllo deve avere il contenuto minimo previsto dall'art. 33 del GDPR e dai provvedimenti in materia emanati dall'Autorità di controllo. La comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui all'art. 34 del GDPR.

I soggetti designati devono opportunamente documentare le violazioni di dati personali subite, anche se non comunicate all'Autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che si intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità di controllo al fine di verificare il rispetto delle disposizioni previste dalla normativa vigente in materia.

Altresì, anche il Responsabile del trattamento di cui all'art. 28 del GDPR è obbligato ad informare il Titolare ed il RPD, tempestivamente e senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione di dati personali.

Art. 16 – Gruppo referenti privacy

Nell'ambito della struttura organizzativa del Comune di Carpi è costituito un gruppo di referenti privacy, con il compito di supportare il Titolare e il RPD nel coordinamento e nella gestione operativa degli adempimenti previsti dalla legislazione vigente in materia di protezione dei dati personali.

Del gruppo referenti privacy fanno parte, oltre ai soggetti designati dal Titolare e i loro delegati, anche eventuali altri referenti individuati dai soggetti designati all'interno dei Settori/Servizi di rispettiva competenza.

Il Titolare, nonché ciascun soggetto designato, agevolano il lavoro del gruppo dei referenti privacy:

- consentendo ai soggetti designati, ai delegati e ai referenti individuati di partecipare a riunioni o gruppi di lavoro tematici, all'interno dell'orario di lavoro;

- favorendo la partecipazione dei soggetti designati, dei delegati e dei referenti a corsi di formazione e/o aggiornamento in materia di protezione dei dati personali;
- facilitando il flusso di comunicazioni interne affinché ciascun delegato e referente sia informato in merito ad ogni cambiamento circa i processi e le attività che possano influire sul trattamento dei dati all'interno del Settore di rispettiva appartenenza.

Art. 17 – Accesso civico generalizzato e protezione dei dati personali

In materia di accesso civico generalizzato e protezione dei dati personali, il RPD funge da supporto ai Settori/Servizi competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti alle richieste di accesso civico generalizzato.

Altresì, il RPD funge da supporto al RPCT nei casi di riesame di istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali.

Inoltre, il RPD, su richiesta dei Settori/Servizi, fornisce il proprio parere in ordine alla valutazione dell'eventuale pregiudizio che l'accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del GDPR.

Il RPD, su richiesta dei Settori/Servizi, fornisce il proprio parere in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi relativi alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Alla luce di tale parere, i Settori/Servizi competenti relativamente alle singole richieste di accesso effettueranno il bilanciamento tra gli interessi lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare.

Art. 18 – Disposizioni finali e rinvio

Il presente modello organizzativo sarà sottoposto a revisione ogni qualvolta si renderà necessario in considerazione dell'evoluzione tecnica e normativa in materia.

Per tutto quanto non espressamente disciplinato con le disposizioni di cui al presente modello organizzativo, si applicano le disposizioni del GDPR e tutte le norme vigenti in materia di protezione dei dati personali.