ROMA

Modello organizzativo capitolino in materia di protezione dati

Linee guida sulla disciplina delle figure del Designato e del Referente e indicazioni operative sull'utilizzo e la gestione digitalizzata dell'applicativo Motore Unico Amministrativo (MUA) e attività correlate

Indice

Introduzione

Con l'emanazione del Regolamento UE n.679/2016 (General Data Protection Regulation – Regolamento Generale Protezione Dati – GDPR), entrato in vigore il 25 maggio 2018, la disciplina che regola la materia della protezione dei dati personali ha seguito un nuovo paradigma capace di elevare il diritto alla protezione dei dati personali a diritto fondamentale e imporre alle pubbliche amministrazioni nuovi obblighi e misure (tecnico organizzative) nell'ottica di garantire una maggior tutela dei diritti degli interessati che, rispetto alla previgente normativa vengono rafforzati.

Tra le principali novità introdotte dalla nuova disciplina vi sono il principio cardine di *accountability* (della responsabilizzazione) e i principi di *privacy by design e by default,* i quali implicano l'applicazione delle tutele di trattamento dei dati sin dalla loro progettazione e per impostazione predefinita.

Con il suddetto Regolamento, si è operato anche un processo di armonizzazione delle legislazioni dei Paesi Europei in materia di protezione dei dati personali nonché di libera circolazione di tali dati all'interno dell'Unione Europea, garantendo, in tal modo, regole comuni per tutti i paesi membri.

Nel nostro paese l'adeguamento alla normativa regolamentare europea è intervenuto a seguito del D. Lgs. n. 101 del 10 agosto 2018 che ha operato molte modifiche alla disciplina previgente di cui al D. Lgs. n.196/2003 (c.d. Codice privacy) nonché l'abrogazione di numerose norme in esso contenute ritenute incompatibili con le nuove disposizioni, introducendo, allo stesso tempo, molteplici rinvii al GDPR da considerarsi come la fonte principale della disciplina sulla protezione dei dati personali.

L'Amministrazione Capitolina con deliberazione della Giunta Capitolina n. 35/2021 ha approvato il *Regolamento sul modello organizzativo in materia di protezione dati* che fa riferimento ad un "modello organizzativo privacy" che adotta un sistema unitario ed omogeneo capace di valorizzare le specificità delle diverse strutture capitoline e le differenti tipologie di trattamento dei dati nonché in grado di identificare i distinti ruoli a presidio delle attività e dei processi organizzativi interni.

Tutto ciò premesso, le presenti *linee guida* hanno l'obiettivo di illustrare, in via generale, le regole di funzionamento del modello organizzativo capitolino al fine di supportare le strutture nella sua attuazione, con riferimento ai diversi ruoli e alle connesse responsabilità che fanno capo alle figure del *designato* e del *referente.* In riscontro al taglio operativo del documento, vengono richiamate alcune informazioni sulle modalità di gestione tramite il sistema MUA (Motore Unico Amministrativo) dei trattamenti più importanti riconducibili alle suddette figure.

Il presente documento, inoltre, illustra, seppur in maniera sintetica, alcuni aspetti della nuova e complessa disciplina che trova negli atti, circolari e materiale informativo pubblicati nella Intranet dell'Ufficio RPD e nelle numerose iniziative formative messe in campo al riguardo dall'Amministrazione, un pratico compendio alla conoscenza della materia che non può, tuttavia, prescindere da un'attenta lettura della normativa di riferimento.

1. Quadro normativo di riferimento

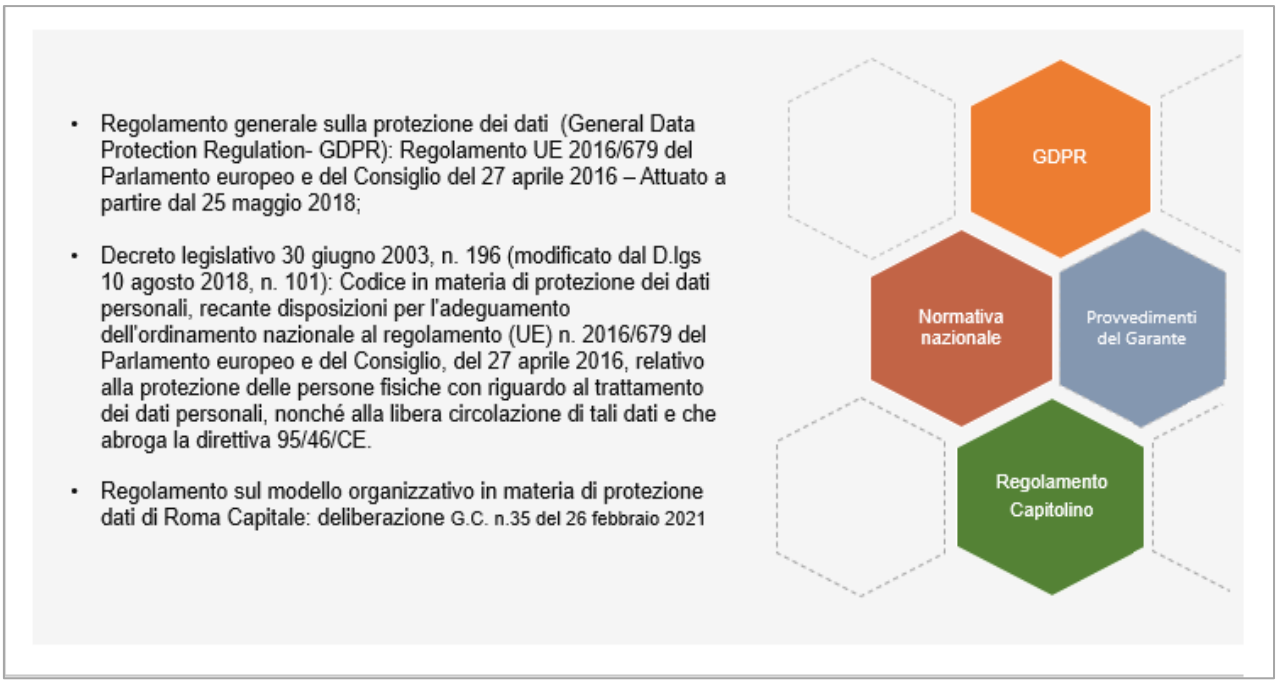
Il quadro normativo che attualmente regola la materia riguardante la protezione dei dati personali si declina nelle disposizioni comunitarie, in quelle nazionali di attuazione e richiama i provvedimenti adottati dal *Garante per la protezione dei dati personali* quale Autorità amministrativa indipendente.

La materia è richiamata anche in altri ambiti normativi, in particolare, quelli sulla trasparenza amministrativa e il diritto di accesso (Legge 241/90 e il D. Lgs. n. 33/2013). Un cenno va fatto anche alla Direttiva UE n. 680/2016 e al D. Lgs. n. 51 del 18 maggio 2018, riguardanti il trattamento nell'ambito di indagini, accertamenti e perseguimento di reati o esecuzione di sanzioni penali, che si applicano ai trattamenti effettuati dall'autorità giudiziaria, ma che può trovare applicazione da parte della Corpo di Polizia Locale nell'ambito dell'esercizio delle funzioni di polizia giudiziaria.

Infine, appare opportuno un riferimento alle "Linee Guida per la formazione, gestione e conservazione dei documenti informatici" adottate con determinazione n. 407/2020 AGID.

Per garantire la corretta attuazione degli obblighi e adempimenti dettati dal GDPR all'interno dell'Ente, l'Amministrazione ha definito, con deliberazione G.C. n. 35 del 26 febbraio 2021, un preciso assetto di responsabilità tenuto conto della specifica organizzazione capitolina.

Sintesi del quadro di riferimento per gli uffici capitolini



2. Cenni sulla nuova disciplina introdotta dal GDPR

2.1 I "Dati personali" e il "Trattamento dei dati"

L'art. 4 del Regolamento UE fornisce una chiara definizione sia dei *dati personali* (con riferimento alle sole persone fisiche) sia del *trattamento dei dati.*

2.1.2 I Dati personali

Per dati personali si intendono le informazioni che identifichino o rendano identificabile (*ossia quando sia possibile individuare una correlazione tra il dato e il soggetto*), direttamente o indirettamente, una persona fisica e che possano fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc... Le nuove tecnologie hanno conferito importanza ad altre tipologie di dati, tra cui quelli relativi alle comunicazioni in rete (indirizzi IP, e-mail, *cookie*) e telefoniche e quelle che consentono la geolocalizzazione.

> Ai sensi dell'art. 4, RGPD, per dato personale si intende "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".

2.1.3 Dati personali particolari (ex dati sensibili)

Si tratta di una particolare categoria di dati disciplinati dall'art. 9 del GDPR, idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

- *Dato Genetico: 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.*
- *Dato Biometrico: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.*
- *Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.*

2.2 Trattamento dei dati (artt. 4-6, 13 GDPR/art. 3 D.G.C. n. 35/21)

Anche in questo caso la definizione di trattamento dati viene fornita dall'art.4 del GDPR. Per trattamento dei dati si intende lo svolgimento di qualsiasi operazione o complesso di operazioni avente ad oggetto la gestione dei dati personali. Costituiscono "trattamento di dati personali" le operazioni di raccolta, registrazione, organizzazione, strutturazione, conservazione, modifica, estrazione, consultazione, diffusione, cancellazione, ecc. …

La liceità (base giuridica che giustifica il trattamento dei dati), la correttezza e la trasparenza sono principi fondamentali del trattamento e della protezione dei dati personali. Il GDPR prevede, inoltre, che il trattamento debba essere adeguato, pertinente, limitato a quanto necessario rispetto alle finalità per le quali è effettuato (principio di minimizzazione dei dati) ed avvenire nel rispetto dei principi di integrità e riservatezza a garanzia della sicurezza dei dati, limitando il rischio di sottoporre i dati a

trattamenti non autorizzati o illeciti, nonché di perdita, distruzione o danneggiamento accidentale degli stessi.

Il trattamento di dati personali nelle pubbliche amministrazioni è considerato lecito se ricorre almeno una delle seguenti condizioni (art. 6 GDPR):
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

I presupposti di liceità sui quali si basa il trattamento dei dati da parte di Roma Capitale sono disciplinati dall'art.3 del Regolamento capitolino.

Ai sensi dell'art. 4, RGPD, il trattamento dei dati consiste in "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**"

Gli Artt. 2-*sexies* (Trattamento di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante) e 2-*septies* (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute) del *Codice in materia di protezione dei dati personali* stabiliscono le modalità di trattamento dei dati personali particolari.

In presenza di un trattamento dei dati deve essere sempre adottata l'informativa (Informativa privacy - artt. 13-14 GDPR) di riferimento. Le informazioni presenti nell'informativa devono essere concise, agevolmente accessibili e di facile comprensione e deve essere usato un linguaggio semplice e chiaro anche in considerazione del fatto che la normativa nazionale prevede che il trattamento dei dati sia lecito anche per il minore che abbia almeno 14 anni.

In adeguamento agli obblighi legislativi in materia di protezione di dati personali, così come previsto dalla normativa vigente e in particolare dal Regolamento (UE) 679/2016 - Regolamento generale sulla protezione dei dati, il Dipartimento Partecipazione, Comunicazione e Pari Opportunità (DPCPO) e l'Ufficio RPD hanno avviato, in collaborazione con il Responsabile della Protezione dei Dati personali (RPD), una serie di attività volte a supportare le Strutture nella revisione e nell'aggiornamento delle informative privacy, sia di natura generale che specifica, da fornire necessariamente agli utenti dei servizi *on-line* del Portale istituzionale di Roma Capitale nonché a tutti i cittadini che fruiscono dei servizi dell'Ente anche attraverso i tradizionali sportelli fisici.

Nel corso di tale attività, l'ufficio RPD ha già provveduto a trasmettere le informative definitive e validate dal DPO con valenza trasversale per tutto l'Ente quali, ad esempio, l'informativa "personale dipendente e collaboratori, "URP, Reclami e relazioni con

l'utenza" o di competenza *ratione materiae* delle strutture *owner* delle funzioni relative ai servizi erogati.

2.2.1 I soggetti coinvolti nel trattamento (art. 4 del GDPR/artt. 4-10 D.G.C. n. 35/21)

La nuova disciplina, rispetto a quella previgente, ha introdotto una nuova configurazione dei soggetti chiamati a trattare i dati personali, che si fonda sul principio di *accountability* che sollecita, da parte dei suddetti soggetti atteggiamenti proattivi a dimostrazione dell'impegno teso all'adozione delle misure più idonee ad assicurare che il trattamento venga effettuato conformemente alle nuove disposizioni normative.

Soggetti coinvolti nel trattamento dei dati personali:

Titolare: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i messi del trattamento di dati personali. Esso è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR:
Contitolari: qualora vi siano due o più titolari del trattamento che determinino congiuntamente le finalità e i messi del trattamento, essi sono contitolari del trattamento;
Responsabile del trattamento: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento sulla base di un contratto o altro atto giuridico;
Sub-responsabile del trattamento: soggetto eventualmente nominato dal responsabile del trattamento ai sensi dell'art. 28, per lo svolgimento di specifiche attività, fermo restando che il responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile;
Designato al trattamento dei dati personali: persona fisica espressamente designata che opera sotto l'autorità del Titolare o del responsabile del trattamento nell'ambito del proprio assetto organizzativo conspecifici compiti e funzioni;
Autorizzato: la persona fisica che ha ricevuto dal Titolare precise istruzioni per l'esecuzione dei trattamenti dati personali all'interno dell'organizzazione dello stesso Titolare e sotto la sua diretta autorità;
Interessato: persona fisica (identificata o identificabile) che fornisce i propri dati personali a un Titolare per le finalità specificate nell'informativa.

Tra le figure introdotte dal GDPR (artt. 37, 38, 39) vi è quella del Responsabile della Protezione dei Dati (RPD o anche DPO - *Data Protection Officer*) la cui designazione, da parte del Titolare o del responsabile del trattamento, è obbligatoria per tutti gli enti pubblici. Il RPD ricopre una funzione di verifica della *compliance* delle azioni e misure adottate alla disciplina dettata dal GDPR e un'attività che si sostanzia, tra l'altro, in compiti di supporto e consulenza al Titolare e di sensibilizzazione e formazione del personale. Funge, inoltre, da punto di riferimento per i soggetti interessati e fra l'Ente e l'Autorità Garante per la protezione dei dati personali.

La disciplina dei soggetti che effettuano il trattamento dei dati personali è stabilita dal *Codice per la protezione dei dati personali* (Titolo IV – parte I).

Il Regolamento capitolino affronta la suddetta disciplina nell'ambito dei contenuti del "Capo II" dedicato al "Modello organizzativo".

2.2.2 *Privacy by Design* e *Privacy by Default* (art. 25 GDPR/art. 6 D.G.C. n. 35/21)

I principi di "*Privacy by Design*" e "*Privacy by Default*" implicano che in fase di progettazione di un'attività che comporti il trattamento di dati personali, il Titolare debba individuare le misure di sicurezza idonee (es: minimizzazione e pseudonimizzazione) alla protezione dei dati, nonché mettere in atto misure tecniche/organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

2.2.3 Registro dei trattamenti (Art. 30 GDPR/artt .12 e 13 D.G.C. n. 35/21)

Il Regolamento prevede, in capo al Titolare e Responsabile, la predisposizione e tenuta di un registro delle attività di trattamento svolte sotto la propria responsabilità, che consenta di avere una panoramica dei trattamenti dei dati personali effettuati all'interno dell'organizzazione funzionale, tra l'altro, all'individuazione dei trattamenti che presentano particolari rischi per i diritti degli interessati.

Il Regolamento capitolino agli artt. 12 e 13 richiama la disciplina relativa, rispettivamente, al "Registro del Titolare del trattamento" indicando i contenuti minimi che il registro deve recare e l'indicazione circa la sua conservazione che viene attribuita all'Ufficio RPD, e al "Registro del Responsabile del trattamento" con l'elenco delle categorie di attività trattate per conto del Titolare e l'indicazione del Designato al trattamento quale soggetto tenutario del registro (art. 6 Regolamento capitolino).

Il Registro dei trattamenti viene gestito e conservato dall'Ufficio RPD con modalità digitali attraverso il sistema MUA.

2.2.4 Misure di Sicurezza (Art. 32 – 34 GDPR/Art.11 D.G.C. n. 35/21)

Per misure di sicurezza si intendono il complesso di misure tecniche e organizzative idonee a garantire un "livello di sicurezza adeguato al rischio". Tra le suddette misure sono ricomprese:

- le tecniche di pseudonimizzazione (art.4, punto 5 GDPR) e di cifratura dei dati personali;
- la capacità di assicurare con continuità la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
- alla capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali nel caso che si verifichi un incidente fisico o tecnico;
- la capacità di adottare procedure volte a testare, verificare e valutare con regolarità l'efficacia delle misure tecniche e organizzative adottate a garanzia della sicurezza del trattamento dei dati.

La suddetta casistica deve intendersi non esaustiva, poiché è rimessa al Titolare (o al responsabile per il trattamento dei dati) la valutazione delle misure idonee da adottare, caso per caso, in rapporto ai rischi che il trattamento comporta.

La conformità al regolamento dei trattamenti effettuati può essere facilitata attraverso l'adesione del Titolare a un codice di condotta o dal ricorso all'istituto della certificazione del sistema di protezione dati come. Al riguardo si richiama l'art. 11 del Regolamento capitolino rubricato "Sicurezza del trattamento".

2.2.5 Valutazione di impatto sulla protezione dei dati (art. 35 GDPR/art. 14 D.G.C. n. 35/21)

Nel GDPR viene affrontato il *rischio inerente al trattamento* (rischio di impatti negativi sui diritti e sulle libertà delle persone interessate), oggetto di un processo di valutazione che volto ad analizzare i rischi e ad individuare le conseguenti misure tecniche e/o organizzative idonee a limitarli. All'esito di detta valutazione il Titolare potrà decidere se iniziare il trattamento (applicando le misure e gli accorgimenti per minimizzare il rischio) ovvero consultare l'Autorità del Garante per ottenere indicazioni su come gestire il rischio residuale. L'Autorità non ha il compito di "autorizzare" il trattamento, bensì solo quello di indicare le misure ulteriori eventualmente da implementare a cura del Titolare.

L'articolo 25, in particolare, introduce il principio di *data protection by design/by default*, ossia declina come sia necessario configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati.

Il principio della protezione dei dati fin dalla progettazione, così come previsto altresì all'art. 14 del Regolamento capitolino, che disciplina l'attuazione della valutazione d'impatto (DPIA) nel caso in cui il Titolare rilevi, prima di effettuare un trattamento – considerati la natura, l'oggetto, il contesto e le finalità dello stesso nonché l'eventuale utilizzo di nuove tecnologie – un rischio elevato per i diritti e le libertà delle persone fisiche, prevede che la protezione dei dati sia integrata nell'intero ciclo di vita della tecnologia e/o del servizio/trattamento, dalla primissima fase di progettazione fino all'utilizzo e all'eliminazione finale.

E' importantissimo tenere conto degli aspetti inerenti alla protezione dei dati ogni qualvolta vengono ideati nuovi servizi, fin dal loro concepimento, anche nel caso di servizi erogati *online* (a tal proposito si veda la Circolare GE/7994 recante il Vademecum sui servizi *online*); questo deve avvenire a monte, non durante o dopo. Prima di procedere al trattamento dei dati vero e proprio va fatta un'analisi preventiva e una serie di attività specifiche e dimostrabili. Tali attività sono connesse al rischio di impatti negativi sulle libertà e i diritti degli interessati che può comportare il trattamento (si leggano i considerando dal 75 al 77 del GDPR); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (valutazione di impatto sulla protezione dei dati, in inglese *Data Protection Impact Assessment* - DPIA) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare il Garante per ottenere indicazioni su come gestire il rischio residuale.

Per un approfondimento della tematica in argomento si invita a prendere visione dell'Allegato 1 al Provvedimento del Garante per la Protezione dei Dati Personali n. 467 dell'11 ottobre 2018 pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018 recante l'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto.

In virtù del combinato disposto degli artt. 32 e 35 del GDPR l'ente svilupperà su ogni trattamento di dati una analisi del rischio e nei casi previsti dalla norma una Valutazione di Impatto. La procedura verrà sviluppata attraverso l'applicativo *software* MUA.
Dal punto di vista operativo, le fasi della procedura saranno le seguenti:

- nel momento in cui dovesse sorgere l'esigenza di avviare una nuova attività, un nuovo servizio, un nuovo procedimento, una nuova funzione oppure modificare degli elementi di trattamenti già mappati in precedenza all'interno del registro (es. software/infrastruttura tecnologica impiegata per l'attività, situazione logistica relativa alle sedi ed agli uffici in cui l'attività verrà sviluppata, soggetti esterni a cui i dati potranno essere comunicati, modalità di svolgimento dell'attività, etc.), il designato al trattamento comunicherà al referente *privacy* tale condizione preventivamente all'avvio della nuova attività/modifica;
- il referente *privacy* avvierà il flusso presente all'interno del sistema MUA inerente alla gestione dei trattamenti (anche oggetto di specifica formazione) e risponderà alle domande che il questionario guidato svilupperà (qualora il referente non fosse in condizione di conoscere alcune informazioni richieste da MUA, nemmeno dopo un confronto all'interno dell'organizzazione di competenza, potrà comunque proseguire con la compilazione delle altre informazioni richieste dal sistema MUA);
- una volta completata la fase di compilazione dati del referente, il sistema MUA ingaggerà l'Ufficio RPD e l'RPD per una verifica dei dati inseriti e la valutazione di alcuni aspetti di natura giuridica inerenti al potenziale nuovo trattamento;
- una volta terminato il passaggio presso l'RPD, il sistema MUA ingaggerà il DTD qualora l'attività descritta abbia delle componenti di natura tecnologica gestite dal Dipartimento medesimo nei confronti del quale il sistema svilupperà una serie di quesiti inerenti agli asset di natura tecnologica che verranno potenzialmente utilizzati nell'attività oggetto di analisi;
- terminato anche il passaggio al DTD, il sistema MUA rielaborerà le informazioni raccolte e produrrà un report con l'esito finale dell'analisi del rischio o della valutazione di impatto (a seconda dei casi);
- il report verrà analizzato dall'ufficio RPD e dall'RPD al fine di verificare l'accettabilità del livello di rischio calcolato oppure la necessità di intervenire per il contenimento di tale livello di rischio, qualora sussistessero le condizioni di cui all'articolo 36, l'RPD consiglierà l'avvio di una consultazione preventiva dell'Autorità Garante;
- l'esito dell'analisi del rischio o della Valutazione di Impatto, incluse le considerazioni dell'Ufficio RPD e dell'RPD, verranno messe a disposizione del Referente *privacy* e del Designato attraverso il sistema MUA, il quale, invierà una mail al referente chiedendo allo stesso di accedere al sistema;
- il Designato al trattamento, al termine dell'istruttoria, deciderà se e quando avviare l'attività/modifica oggetto dell'istruttoria.

2.2.6 Violazione dei dati personali (Artt. 33 e 34 GDPR/art. 15 D.G.C. n. 35/21)

Per violazione del dato si intende la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, che si produce in maniera accidentale o in modo illecito (componente di natura dolosa).

Alla violazione dei dati personali è riferita la procedura dei *Data Breach*. Nel caso di *violazione dei dati personali* la stessa deve essere oggetto di notifica da parte del Titolare all'Autorità Garante, possibilmente entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il Titolare reputi improbabile che la violazione possa costituire un rischio per i diritti e le libertà delle persone fisiche interessate. Qualora la notifica all'Autorità non venga effettuata entro 72 ore, essa deve essere corredata dalla descrizione dei motivi alla base del ritardo.

La procedura concernente la violazione dei dati richiamata dall'art. 15 del Regolamento capitolino, viene gestita attraverso l'applicativo MUA.
I casi in cui sarà necessario applicare la presente procedura sono, a titolo esemplificativo e non esaustivo:

- sottrazione di credenziali di autenticazione;
- furto di PC, Notebook, Tablet, Smartphone contenente dati personali;
- erronea diffusione, pubblicazione, comunicazione di dati personali;
- intrusione non autorizzata nei locali in cui sono conservati/archiviati dati personali;
- furto di archivi cartacei e/o digitali;
- accesso non autorizzato nel sistema informativo;
- azione di malware (virus, etc.) che siano riusciti ad eludere le misure di sicurezza aziendali;
- smarrimento di dati personali (archiviati su supporti cartacei e digitali);
- distruzione di dati personali (archiviati su supporti cartacei e digitali);
- ecc..

Sarà la struttura organizzativa che avrà rilevato l'evento a farsi carico di avviare il flusso "*data breach*" presente all'interno dell'applicativo MUA, tranne nei casi in cui tale evento riguardi i sistemi di elaborazione gestiti centralmente dal DTD o i sistemi di fornitori per i quali il rapporto è gestito direttamente dal DTD. In tali casi, infatti, indipendentemente da chi abbia rilevato l'evento, sarà il/i referente/i privacy del DTD ad avviare il flusso MUA.

Il soggetto che rileverà l'evento dovrà rivolgersi al referente *privacy* della propria struttura organizzativa trasmettendo tutte le informazioni in proprio possesso al fine di consentire al referente medesimo di compilare il questionario guidato che l'applicativo MUA proporrà.
La gestione della violazione concreta, potenziale o sospetta, prevede l'attuazione delle seguenti attività:

A. rilevazione della violazione dei dati personali;
B. raccolta di informazioni sulla violazione;
C. comunicazione della violazione al Referente p*rivacy* della struttura/dell'Ente che procederà ad una prima analisi della violazione di concerto con il Designato al trattamento della struttura organizzativa;
D. compilazione della prima parte del flusso di *data breach* fino a chiusura della sezione (step A-B-C);
E. compilazione da parte del RPD/Ufficio RPD della seconda parte del flusso e valutazione della necessità di effettuare la comunicazione all'Autorità Garante;
F. notifica all'Autorità Garante della violazione subìta, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche;
G. eventuale comunicazione della violazione di dati personali all'interessato nel caso vi sia un rischio elevato (il documento per la segnalazione agli interessati potrà essere generato tramite il flusso dei "*data breach*");
H. nel caso in cui si sia valutato di non effettuare comunicazione all'Autorità Garante, sarà necessario registrare la violazione all'interno del sistema MUA, tramite lo svolgimento del flusso di segnalazione di *data breach*, al fine di mantenere aggiornato il "Registro degli incidenti". Tale registro, sarà reperibile all'interno del sistema nella pagina "Elementi di analisi", alla voce "Regolamento 679/2016/UE - d*ata breach*".

Le fasi specifiche della procedura all'interno del sistema MUA sono le seguenti:

1. Il Referente *privacy* dovrà rispondere alle domande del questionario presenti in MUA relative a:
   - identificazione e descrizione dell'evento;
   - misure tecnologiche e organizzative applicate a protezione dei dati (prima, durante e dopo la violazione);
   - informazioni relative ai soggetti individuati per la gestione della procedura (se necessario dovrà farsi affiancare nella sua compilazione da coloro che sono in possesso delle informazioni);
2. conclusa la compilazione del questionario, il Referente chiuderà il flusso, completandolo e passando l'incarico all'ufficio RPD ed all'RPD;
3. il flusso incarica l'ufficio RPD e l'RPD dello svolgimento della seconda parte del flusso;
4. l'ufficio RPD e l'RPD ricevono una mail dal sistema MUA che informa della necessità di proseguire l'istruttoria del *data breach*;
5. l'Ufficio RPD e l'RPD analizzano, all'interno del sistema MUA, le informazioni inserite durante la prima parte del flusso;
6. in base alle informazioni inserite, l'RPD valuta la necessità di fare comunicazione all'Autorità Garante e agli interessati e procede con la compilazione del questionario;
7. l'Ufficio RPD e l'RPD procedono alternativamente fino alla chiusura del flusso in MUA.

7.1. Caso A: **incidente da inserire nel registro incidenti**

7.1.1. inserimento della violazione nel registro incidenti

7.1.2. comunicazione da parte dell'Ufficio RPD o dell'RPD di chiusura dell'incidente

7.2 Caso B: **incidente da inserire nel registro incidenti e da notificare all'Autorità Garante (nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche)**

7.2.1 inserimento della violazione nel registro incidenti;

7.2.2 generazione del modulo di comunicazione di *data breach*, che viene firmato dall'autore (direttore dell'ufficio RPD o RPD) con il sistema di firma MUA;

7.2.3 trasmissione della comunicazione di chiusura della procedura;

7.2.4 acquisizione mediante *download* del modulo di segnalazione all'Autorità Garante nel seguente modo:

- accedere alla sezione "Elementi d'analisi" alla voce "Regolamento 679/2016/UE - Data breach";
- posizionarsi sulla violazione/incidente inserito;
- espandere la sezione "File allegati";
- cliccare sul documento da scaricare denominato "Modello di comunicazione al Garante-Data breach";
- la documentazione viene inviata anche mezzo mail agli

indirizzi indicati durante lo svolgimento del flusso;

7.2.5 sottoscrizione digitale (con firma elettronica qualificata/firma digitale) o con firma autografa (in questo caso il documento deve essere presentato unitamente alla copia del documento di identità del firmatario) da chi effettua la comunicazione;

7.2.6 protocollazione del documento;

7.2.7 invio tempestivo del documento a mezzo PEC all'indirizzo protocollo@pec.gpdp.it. L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e, opzionalmente, la denominazione del Titolare del trattamento;

***7.3 Caso C*: incidente da inserire nel registro incidenti, da notificare all'Autorità Garante e da comunicare agli interessati (nel caso in cui la violazione comporti un rischio elevato per i diritti e la libertà delle persone fisiche)**

7.3.1 inserimento della violazione nel registro degli incidenti e invio notifica all'Autorità Garante come da punti da 7.2.1 a 7.2.7;

7.3.2 comunicazione della violazione di dati personali all'interessato.

Vengono di seguito descritte le informazioni che il flusso MUA richiederà di compilare:

Step A. Identificazione e descrizione dell'evento:

Indicare la tipologia di comunicazione che si sta facendo all'Autorità Garante. Il flusso chiederà che tipo di notifica si sta effettuando:

- preliminare (il Titolare del trattamento avvia una procedura di segnalazione senza avere un quadro completo della violazione e si riserva di effettuare una successiva notifica integrativa);
- completa;
- integrativa (il Titolare del trattamento integra una precedente modifica). Nel caso di notifica integrativa, il flusso permetterà di importare le informazioni di quella preliminare. Se noto, il flusso richiederà il numero di fascicolo assegnato alla precedente notifica dall'Autorità Garante.

Selezionare gli strumenti *hardware*, *software* o locali fisici oggetto della violazione/incidente (se il sistema non è ancora stato popolato con queste informazioni, il flusso permetterà di inserire l'elemento che ha subìto la violazione). Se associati, il sistema permette di indicare quali trattamenti collegati all'elemento violato sono stati oggetto della violazione.

Nel caso in cui i collegamenti non siano stati ancora effettuati, il flusso dà la possibilità di indicare i trattamenti oggetto di violazione.

Descrivere l'evento che ha condotto alla violazione subìta.

Indicare quando è avvenuta la violazione.

Indicare la data e l'ora in cui il Titolare del trattamento è venuto a conoscenza della violazione.

Indicare le modalità con le quali il Titolare è venuto a conoscenza della violazione (per il tramite del responsabile del trattamento o in altro modo).

Indicare se nel trattamento sono coinvolti ulteriori soggetti esterni. Il flusso permette di scegliere un soggetto tra quelli presenti in elenco "Enti Esterni" oppure di inserire un nuovo soggetto.

Le informazioni che dovranno essere inserite sono:

- denominazione (indicare il nome e cognome in caso di persona fisica)
- Codice fiscale/Partita Iva;
- ruolo: Co-titolare, Responsabile esterno ai sensi dell'Art. 28, Rappresentante del Titolare non stabilito nell'Ue.

Indicare le possibili cause della violazione. Scegliere fra le possibilità presenti:

- Azione intenzionale interna;
- Azione accidentale interna;
- Azione intenzionale eterna;
- Azione accidentale esterna;
- Sconosciuta;
- Altro.

Scegliendo "Altro", il flusso permette di indicare altre possibili cause della violazione.

Indicare la natura della violazione scegliendo una o più delle seguenti risposte:

- Perdita di confidenzialità (diffusione/accesso non autorizzato o accidentale);
- Perdita di integrità (modifica non autorizzata o accidentale);
- Perdita di disponibilità (impossibilità di accesso, perdita, distruzione non

autorizzata o accidentale).

Per ognuna delle risposte selezionate, il flusso chiede di specificare ulteriormente la natura della violazione e indicare le possibili conseguenze della violazione sugli interessati (è possibile selezionare più di una risposta)

Indicare il volume dei dati violati (ad esempio il numero di referti, numero di *record* di un *database*, numero di transizioni registrate).

Se il numero non è conosciuto, selezionare la voce “Un numero (ancora) non definito di dati”.

Indicare il numero di interessati coinvolti nella violazione.

Se il numero non è conosciuto selezionare la voce “Un numero (ancora) sconosciuto di interessati”.

Indicare le possibili categorie di interessati coinvolte nella violazione.

Nel caso in cui precedentemente siano stati individuati i trattamenti oggetto della violazione, il sistema riproporrà le relative categorie di interessati.

Nel caso in cui non siano stati selezionati i trattamenti, sarà necessario indicare le possibili categorie d’interessati, scegliendo dal menù in elenco (è possibile selezionare più di una risposta).

Step B: Misure tecnologiche e organizzative applicate a protezione dei dati (prima, durante e dopo la violazione)

Indicare le misure tecnologiche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti nella violazione.

Indicare le misure tecniche e organizzative adottate (o di cui si propone l’adozione futura) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati.

Nella descrizione, distinguere fra le misure già adottate e quelle in corso di adozione.

Indicare le misure tecniche e organizzative adottate (o di cui si propone l’adozione futura) per prevenire simili violazioni future.

Step C. Ulteriori informazioni

Indicare il nominativo del soggetto deputato all'invio della notifica al Garante (scegliere nel menù in elenco). Nel caso in cui queste informazioni non siano presenti nel sistema, verranno richieste.

- Cognome e nome del segnalante;
- E-mail;
- Recapito telefonico per eventuali comunicazioni;
- Funziona rivestita.

Dati relativi al Titolare del trattamento

- Denominazione;
- Codice fiscale/Partita Iva;
- Stato;
- Indirizzo;
- CAP;
- Città;
- Provincia;
- E-mail;
- Pec.

Il flusso incarica l'ufficio RPD e l'RPD dello svolgimento della seconda parte del flusso. Coloro che verranno incaricati riceveranno una comunicazione tramite mail dell'avvenuto incarico.

Se le persone incaricate fossero più di una, il primo che avvierà il flusso ne otterrà l'incarico esclusivo notificando agli altri utenti l'avvenuta presa in carico.

Step D. Comunicazione della violazione

In base alle informazioni inserite, l'RPD valuta la necessità di fare comunicazione all'autorità Garante. Qualora si voglia notificare la violazione al Garante, il sistema genera il documento sulla base del modello predisposto dall'Autorità Garante.

In ogni caso, il sistema registra tutte le informazioni al fine di implementare il registro delle violazioni

Indicare se la comunicazione è effettuata ai sensi:

- Dell'Art.33 Gdpr;
- Dell'Art. 26 D.Lgs 51/2018

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione.

Nel caso in cui sia stato individuato il DPO, indicare il numero di protocollo assegnato alla comunicazione all'Autorità Garante dei dati di contatto del DPO.

In alternativa, indicare il soggetto da contattare:

- Cognome e Nome;
- E-mail;
- Recapito telefonico per eventuali comunicazioni;
- Funzione rivestita.

Nel caso in cui la comunicazione venga effettuata oltre le 72 ore, il flusso chiederà di motivare il ritardo.

Descrivere l'incidente alla base della violazione.

Descrivere le categorie di dati personali oggetto della violazione.

Indicare tipologie di dati coinvolti nella violazione.
Se durante la prima parte del flusso sono stati selezionati dei trattamenti, il flusso leggerà e preselezionerà le tipologie di dati già indicate sul trattamento.

Indicare, per ogni tipo di dato scelto o collegato ai trattamenti coinvolti nella violazione, le specifiche categorie di dati.

Indicare la stima della violazione.

Indicare le motivazioni della scelta.

Step E. Comunicazione agli interessati

Indicare i potenziali effetti negativi sugli interessati della violazione.

- Se si seleziona uno dei rischi in elenco, il flusso chiederà di indicare se ci sono delle motivazioni per cui non deve essere fatta comunicazione agli interessati. Per ognuna delle voci selezionate indicare le motivazioni.
- Se tra le voci si seleziona "Nessun rischio", il flusso dirà che non vi è necessità di fare comunicazione agli interessati.
- Se si seleziona uno dei rischi presente in elenco, ma se non sono presenti le condizioni per cui non vi è necessità di fare comunicazione, il flusso indicherà che vi è la necessità di effettuare la comunicazione agli interessati.

Nel caso si sia presa la decisione di effettuare la comunicazione agli interessati, inserire il testo della comunicazione che si intende dare agli interessati.

Nel caso si sia presa la decisione di effettuare la comunicazione agli interessati, indicare la modalità con cui è stata data o si darà comunicazione agli interessati.

Nel caso si sia presa la decisione di effettuare la comunicazione agli interessati, il flusso genererà il documento da inviare agli interessati.

Nel caso si sia presa la decisione di fare comunicazione all'Autorità Garante verrà generato il modulo di comunicazione di *data breach*, che dovrà essere firmato con il sistema di firma MUA.

Il flusso invierà la documentazione generata agli indirizzi mail dichiarati. La documentazione generata sarà scaricabile accedendo alla sezione "Elementi d'analisi" alla voce "Regolamento 679/2016/UE - *Data breach"*, selezionare l'evento per cui si intende scaricare la documentazione, che sarà presente nella sezione "File allegati".

Nel caso in cui sia stato valutato di non effettuare la notifica all'Autorità Garante, verrà comunque inviata notifica della conclusione del flusso e della decisione di non fare comunicazione all'Autorità Garante.

Indicare gli indirizzi e-mail a cui sarà inviata l'eventuale documentazione generata dal flusso e la comunicazione di conclusione del flusso.

Step F. Chiusura dell'incidente

Descrivere il modo di risoluzione della violazione/incidente, nel caso sia stato risolto.

Indicare la data di risoluzione della violazione/incidente, nel caso sia stato risolto.

3. Modello organizzativo capitolino – Le figure del Titolare, Designato e del Referente

In un'ottica di adeguamento alle disposizioni dettate dal GDPR e dal *Codice per la protezione dei dati personali*, Roma Capitale, con deliberazione della G.C. n. 35 del 26 febbraio 2021, ha approvato il Regolamento sul modello organizzativo in materia di protezione dati.

Con il Regolamento capitolino è stato individuato il modello organizzativo (di gestione e di controllo) per la protezione dei dati personali che, tra l'altro, definisce i vari livelli di responsabilità ed i relativi compiti e ruoli.

Tale modello costituisce presupposto fondamentale a garanzia dell'osservanza dei princìpi sulla protezione dei dati e del rispetto degli obblighi di trasparenza, in grado di consentire la puntuale definizione delle responsabilità correlate ai diversi ruoli assunti da ciascun soggetto nell'ambito dell'amministrazione capitolina.

I processi che compongono il modello organizzativo, definiti sulla base di quanto stabilito dal GDPR, possono essere riassunti come segue:

1) Individuazione e nomina dei soggetti "Designati" da parte del Titolare	6) Gestione informative e consensi
2) Individuazione dei Referenti protezione dati	7) Gestione delle richieste degli interessati
3) Individuazione degli Autorizzati al trattamento dei dati	8) Gestione analisi del rischio e valutazione di impatto
4) Gestione dei rapporti con i soggetti terzi con cui si condividono i dati	9) Gestione *Privacy by design* e *by default* per acquisti software/app ecc. …
5) Gestione registro dei trattamenti	10) Gestione *Data Breach*

3.1 Strutture di riferimento

Ufficio Responsabile per la protezione dei dati

I compiti attribuiti all'Ufficio sono dettagliatamente indicati nell'art.10 del Regolamento capitolino.

In particolare, l'Ufficio presta le seguenti attività:

- di supporto nei confronti:
  - delle strutture capitoline per la corretta implementazione del modello organizzativo e per la gestione del sistema digitale di riferimento (MUA) anche attraverso l'elaborazione di linee operative;
  - del Responsabile per la protezione dei dati (RPD) nel rapporto con le strutture capitoline in materia di adeguamento alle disposizioni del GDPR;
- di coordinamento dei Referenti per la protezione dati;
- gestione del registro dei trattamenti e conservazione;
- gestione analisi rischio e valutazione d'impatto;
- gestione *data breach*.

Il Dipartimento Partecipazione, Comunicazione e Pari Opportunità

Il dipartimento nel suo ruolo di *struttura competente in materia di comunicazione e di governance dei servizi offerti alla cittadinanza* nell'ambito delle funzioni indicate all'art. 16 del Regolamento capitolino e fatti salvi eventuali ulteriori competenze che possono essere direttamente attribuite alla struttura dal Titolare del trattamento, svolge un'attività:

- di coordinamento e supporto nei confronti delle strutture capitoline con riferimento all'attività di aggiornamento dei contenuti e delle Informative privacy presenti sul portale istituzionale;
- di formulazione di criteri e modelli, concordati con l'Ufficio RPD, per la definizione dei processi e/o requisiti funzionali dei servizi digitali inerenti all'analisi del rischio e la valutazione d'impatto sulla protezione dati.

Il Dipartimento Trasformazione Digitale

Il Dipartimento nel suo ruolo di *struttura competente in materia di trasformazione digitale*, nell'ambito delle funzioni indicate all'art. 17 del Regolamento capitolino e fatti salvi eventuali ulteriori competenze che possono essere direttamente attribuite alla struttura dal Titolare del trattamento, svolge attività di supporto nella valutazione degli aspetti tecnologici relativamente all'impatto di questi sulle attività di trattamento e di sviluppo delle componenti tecnologiche inerenti l'analisi del rischio e della valutazione di impatto secondo modelli e criteri concordati con l'Ufficio RPD e con lo stesso RPD.

3.2 Motore unico amministrativo (MUA)

Si tratta di un *software* adottato dall'Amministrazione Capitolina per la gestone digitale del complesso degli adempimenti resi obbligatori dall'attuale disciplina in materia di protezione dei dati personali, consentendo di predisporre, sottoscrivere elettronicamente, inviare e mantenere aggiornata la relativa documentazione (interna ed esterna – lettere di incarico, informative, consensi, comunicazioni di violazioni, *ecc*. …) in conformità alle disposizioni vigenti con riguardo alle diverse attività di trattamento dati e alle diverse strutture e figure di riferimento. Il sistema, oltre ad automatizzare le principali procedure in uso ed a produrre il complesso dei documenti richiesti dalla più volte richiamata normativa, gestisce tutte le attività di controllo, monitoraggio e consulenza di competenza del RPD.

In particolare, il MUA riporta, al suo interno, l'elenco riguardante le diverse tipologie dei trattamenti, alcuni dei quali già presenti di *default* nel programma, altri che possono essere oggetto di integrazione da parte delle diverse figure preposte al sistema in ragione del ruolo ricoperto.

In sintesi, per ciascuna tipologia di trattamento, il sistema prevede: *le caratteristiche di riferimento, la tipologia di supporto, la natura dei dati, la finalità del trattamento, le categorie degli interessati, altre caratteristiche che possono essere implementate liberamente dalle figure abilitate nonché i procedimenti amministrativi correlati* essendo disponibile sul sistema la *mappatura completa dei procedimenti capitolini* (di istanza di parte e d'ufficio) di recente predisposizione a cura dell'Ufficio RPD. Ciò consente di rendere il più possibile automatizzata l'intera procedura e di gestire al meglio i concetti introdotti dal GDPR di *privacy by default e privacy by design* con riguardo a ciascuna tipologia di trattamento.

Il Sistema individua, inoltre, le persone coinvolte nel trattamento, i *software* e gli strumenti informatici utilizzati, i luoghi fisici o le sedi degli uffici all'interno dei quali sono conservati documenti cartacei che riportano i dati personali inerenti al trattamento considerato.

Le indicazioni circa le funzionalità e le modalità di utilizzo del sistema MUA sono fornite attraverso una specifica formazione, con didattica in modalità *eLearning* (aule virtuali in modalità sincrona), rivolta alle diverse figure coinvolte nelle attività di trattamento. Si rappresenta, inoltre, che, a supporto del personale preposto alla gestione del sistema MUA, è stato attivato un servizio di *help desk* (06/56548302 - assistenzamotoreunicoamministrativo.it), mentre la relativa manualistica è consultabile all'interno dello spazio Intranet dell'Ufficio RPD unitamente alle circolari e a materiale didattico e, comunque, di interesse.

3. 3 Lo schema dei ruoli previsti

Le figure chiave per l'attuazione della disciplina in esame presenti nella struttura organizzativa del Titolare sono, soprattutto, quelle del Designato, al quale sono attribuiti i compiti previsti dall'art. 6, comma 3 del Regolamento capitolino e del Referente che è incaricato dell'attività di supporto al Designato nello svolgimento delle attività relative al trattamento dei dati ed i cui compiti sono disciplinati all'art. 7 del suddetto Regolamento.

3.3.1 Titolare e soggetti designati

Per Titolare dei dati personali si intende Roma Capitale in persona del Sindaco *pro-tempore* (art. 4 del Regolamento capitolino).

L'articolo 24 del GDPR stabilisce che: *"tenuto conto 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, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario"*

In forza del principio della *accountability* (responsabilizzazione), il Titolare del trattamento deve essere in grado di poter dimostrare di aver adottato misure organizzative, tecniche e di sicurezza idonee alla protezione dei dati e che queste misure siano state, con continuità, oggetto di riesame ed eventuali aggiornamenti.

Prioritariamente rientrano tra le responsabilità del Titolare e dei Responsabili: l'attuazione delle prassi di *privacy by design/default*, la valutazione d'impatto, la definizione e il mantenimento delle procedure di sicurezza e valutazione dei rischi, la tenuta dei rispettivi registri delle attività di trattamento, la valutazione prudenziale sulla violazione dei dati personali, del coefficiente di gravità e delle relative ricadute sul soggetto interessato.

Nel rispetto di quanto stabilito dal GDPR, l'articolo 2-*quaterdecies*, comma 1, del *Codice per la protezione dei dati personali*, attribuisce al Titolare la facoltà di conferire, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, specifici compiti e funzioni connessi al trattamento di dati personali a persone fisiche che operano sotto la sua autorità.

In ossequio alle suddette disposizioni la Giunta Capitolina con deliberazione G.C. 35/2021 ha dato mandato al competente Dipartimento Organizzazione e Risorse Umane di adeguare gli artt. 30, comma 1 lett. g) e 31, comma 2, lett. a) del *Regolamento*

sull'Ordinamento degli Uffici e Servizi di Roma Capitale, rispettivamente rubricati "Direttore di Dipartimento o Struttura analoga" e "Direttore di Municipio", inserendo, in sostituzione del richiamo all'art. 28 del Regolamento UE 2016/679, la disposizione concernente la responsabilità del **Dirigente apicale "*quale Designato* *al trattamento dei dati, di tutti i trattamenti di dati personali effettuati dall'articolazione organizzativa di competenza, al fine di mettere in atto tutte le misure tecniche e organizzative necessarie per garantire la piena conformità al GDPR*".

Pertanto, nell'ambito del modello organizzativo di cui alla deliberazione G.C. n. 35/2021, i dirigenti che rivestono i ruoli apicali delle diverse strutture in cui si articola l'assetto organizzativo dell'Ente, assumono il ruolo di "**Designati** al trattamento dei dati". L'ordinanza sindacale, oltre a procedere alla suddetta nomina elenca i compiti che fanno capo alla figura del Designato richiamando espressamente quanto previsto all'art.6, comma 3 del Regolamento capitolino:

- verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
- disporre l'attuazione dei provvedimenti emessi dal garante collaborare con il responsabile della protezione dei dati al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
- individuare i soggetti autorizzati al trattamento per la struttura organizzativa di competenza e attribuire loro specifici compiti e attività di protezione dei dati;
- individuare ed incaricare i referenti protezione dati di cui all'articolo 7 del regolamento per la propria struttura organizzativa;
- individuare il personale della propria articolazione organizzativa da sottoporre alle attività formative in materia di protezione dei dati;
- adottare soluzioni di *privacy by design* e *by default* ovvero di protezione dei dati fin dalla progettazione e per impostazione predefinita prevedendo già dall'origine, in considerazione del contesto complessivo ove il trattamento si colloca e dei rischi stimati, un paradigma di trattamento e misure di protezione prefissate;
- procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza e aggiornare i contenuti in materia di protezione dati presenti nella modulistica relativa la propria struttura organizzativa;
- individuare e nominare i responsabili di trattamento e conservare il relativo registro delle attività predisporre in accordo con l'Ufficio RPD un calendario di audit da svolgere congiuntamente con i responsabili del trattamento nominati individuati a campione ovvero a rotazione;
- adottare, se necessario, specifici di disciplinare i tecnici di settore anche congiuntamente con altri designati e/o responsabili del trattamento per stabilire dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla specifica area di competenza;
- fornire riscontro alle richieste dell'interessato per i trattamenti di dati di competenze della propria struttura organizzativa rilevare comunicare i casi di violazione dei dati personali nell'ambito organizzativo di riferimento.

Detta nomina (Ordinanza Sindacale n. 88 del 14/05/2021) ha durata pari a quella già prevista per l'incarico di Direttore apicale, salvo eventuale revoca disposta dal Titolare del trattamento ovvero fino all'interruzione del rapporto di lavoro o di eventuali e/o diversi accordi tra le parti.

Il ruolo di designato è valorizzato nel sistema MUA per ciascun designato. L'atto di nomina dei designati è rinvenibile all'interno del sistema MUA nella scheda/fascicolo di ciascun dirigente apicale presente nel sistema.

Nell'ambito delle suddette attribuzioni, di seguito vengono fornite alcune indicazioni di dettaglio utili ai fini operativi:

1) **Identificazione dei rapporti intercorrenti con soggetti terzi in materia di protezione dati**.
   Tale identificazione avviene a seguito di parere dell'Ufficio RPD e porta alla sottoscrizione di atti di nomina per i Responsabili esterni del trattamento, alla stipula di accordi di contitolarità oppure alla statuizione di titolarità autonome. In ambito operativo sono i Referenti protezione dati nominati dal Designato che, su *input* di quest'ultimo, attivano attraverso il sistema MUA la procedura di richiesta di parere al suddetto Ufficio, il quale vaglierà la situazione ed individuerà la tipologia di rapporto in modo da consentire al sistema di produrre i contenuti in termini di *data protection* corrispondenti alla tipologia di rapporto individuata.

   Nel ruolo dei Responsabili esterni (art.28 GDPR), a titolo esemplificativo, possono essere ricompresi: i fornitori di beni e servizi che trattano per conto del Titolare/Designato dati personali, i soggetti terzi con i quali vengono stipulati protocolli, convenzioni (es. servizio di tesoreria), ecc..., qualora siano autorizzati ad accedere ai dati personali in possesso di Roma Capitale e sempreché detti dati siano trattati per suo conto.

   Qualora il trattamento dei dati avvenga nell'ambito di un contratto di servizio tra Roma Capitale e le società *in house*, ricorre l'obbligo della nomina di queste ultime quali Responsabili esterni (come già avvenuto per alcuni servizi svolti da AMA SpA, Aequa Roma, Roma Servizi per la Mobilità, ecc.).

   Si ritiene utile un cenno alla figura del Medico competente disciplinata dal D.Lgs. n. 81/2008 (*Testo unico in materia di tutela della salute e della sicurezza nei luoghi di lavoro*) ed al suo possibile inquadramento in qualità di responsabile esterno del trattamento sotto l'autorità del Titolare/Designato quale datore di lavoro. Al riguardo l'Autorità Garante ha dissipato ogni dubbio affermando l'autonomia dei trattamenti effettuati dal professionista "*in qualità di autonomo Titolare del trattamento*" per le finalità indicate dalla sopra richiamata disciplina di settore.

2) **Richiesta agli uffici preposti alla valutazione sulla protezione dei dati inerente nuove attività/progetti/servizi preventivamente all'avvio di questi ultimi**
   Tale compito consiste nell'effettuare una preventiva richiesta di valutazione degli aspetti *data protection* inerenti una nuova attività/progetto/servizio al fine di valutarne l'applicazione dei principi di *privacy by design e privacy by default* (si richiama la circolare AR/490/2019). Da un punto di vista prettamente operativo l'input della richiesta è dato dal soggetto Designato e posto in essere dal Referente Protezione Dati. La procedura viene sviluppata mediante il sistema MUA. Per quanto riguarda gli "aspetti tecnologici" la procedura prevede il coinvolgimento delle strutture di cui agli artt.12 e 13 del Regolamento capitolino (attuali DPCPO e DTD). L'Ufficio RPD rilascia apposito parere attraverso il medesimo sistema MUA, al fine di fornire tutte le indicazioni necessarie in termini di *data protection*. A fronte del parere

dell'Ufficio RPD/RPD, il Designato assume le sue decisioni in merito all'avvio o meno del nuovo progetto/servizio/ecc. …

3) **Procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza della propria struttura organizzativa**
   Da un punto di vista prettamente operativo l'input della richiesta viene sviluppata dal Designato e posto in essere dal Referente Protezione Dati. La procedura è sviluppata e gestita mediante il sistema MUA. Il Referente procede all'aggiornamento del *Registro dei trattamenti* attraverso l'ausilio del medesimo sistema e qualora dalla modifica effettuata dovessero conseguire ulteriori attività di *compliance* le comunicherà all'Ufficio RPD. La procedura è la medesima già descritta al paragrafo 2.2.5 inerente la valutazione di impatto e l'analisi dei rischi in quanto ogni potenziale modifica intervenuta ad un trattamento potrebbe comportare la rivalutazione del rischio.

4) **Ricezione e risposta alle richieste dell'Interessato inviate direttamente alla Struttura organizzativa di competenza**
   La richiesta ricevuta dall'interessato è inviata dal Designato all'Ufficio RPD per il tramite del Referente Protezione Dati, il quale attua la relativa procedura attraverso il sistema MUA.
   L'RPD procede alla verifica della richiesta ed al rilascio di apposito parere che viene inviato al Designato attraverso l'ausilio del medesimo sistema. A fronte del parere del RPD, il Designato provvede a rispondere all'Interessato.

5) **Prestazione dell'informativa all'Interessato**
   Tale compito consiste nel prestare agli Interessati idonea informativa per i trattamenti di dati di competenza della propria Struttura Organizzativa. Le informative sono opportunamente verificate e/o proposte dall'Ufficio RPD a fronte di richiesta del Designato per il tramite del Referente Protezione Dati. Nel caso di nuove attività in fase di avvio, l'informativa viene proposta dall'Ufficio RPD/RPD in fase di rilascio del parere attraverso il sistema MUA.

6) **Aggiornamento contenuti privacy modulistica di competenza della propria Struttura organizzativa**
   Tale compito consiste nell'aggiornare i contenuti in termini di *data protection* della modulistica di competenza della propria struttura organizzativa. La modulistica viene verificata e/o proposta dall'Ufficio RPD a fronte di richiesta del Designato per il tramite del Referente. Nel caso di nuove attività in fase di avvio i contenuti *data protection* della modulistica sono proposti dall'Ufficio RPD in fase di rilascio del parere attraverso il sistema MUA.

7) **Individuazione del personale della propria Struttura Organizzativa da sottoporre ad attività formativa in materia di protezione dei dati**
   Tale compito consiste nell'individuazione del personale afferente alla propria struttura organizzativa da inserire in appositi percorsi formativi in materia di *data protection*. Le tipologie di profili ai quali dovrà appartenere il personale selezionato sono individuate dall'Ufficio RPD.

8) **Individuazione dei soggetti "Autorizzati" al trattamento e verifica della loro attività**.
   Tale compito consiste nell'individuazione del personale che può accedere ai dati personali trattati dalla struttura organizzativa di competenza. La formalizzazione dell'incarico ai soggetti autorizzati avviene su *input* del Designato, il quale provvede a sottoscrivere gli atti di nomina con firma

elettronica avanzata. La relativa procedura viene istruita dal Referente utilizzando il sistema MUA.
Il primo avvio della procedura MUA svilupperà massivamente tutti gli atti di nomina dei soggetti che saranno stati individuati come Autorizzati per i singoli trattamenti. Una volta che il sistema sarà entrato a regime attraverso dei connettori con i sistemi *software* dell'ente che detengono l'anagrafica del personale, il sistema MUA importerà eventuali modifiche intervenute al personale e le sottoporrà al Referente per una conferma delle stesse al fine di poter avviare automaticamente il processo di generazione degli atti di nomina.
Il Designato sottoscrive i suddetti atti di nomina attraverso il sistema MUA e ha il compito di vigilare che i soggetti autorizzati nell'ambito della propria struttura operino nel rispetto delle istruzioni impartite.
L'ufficio RPD darà comunicazione ai Referenti ed ai Designati del momento in cui occorrerà avviare la generazione e la sottoscrizione degli atti di nomina all'interno del sistema MUA.

9) **Individuazione Referenti Protezione Dati**
Tale compito consiste nell'individuazione dei Referenti Protezione Dati per la Struttura Organizzativa di competenza. L'attività di formalizzazione dell'incarico avviene su input del Designato, il quale provvede a sottoscrivere gli atti di nomina attraverso il sistema MUA e secondo la procedura indicata nel presente documento (pag. 26).

10) **Rilevazione e comunicazione *data breach***
Tale compito consiste nel procedere alla rilevazione dei *data breach* inerenti alla propria unità organizzativa e l'attivazione dell'apposita procedura *software* attraverso il MUA. Al termine della procedura ed ottenuto il parere del RPD (sempre attraverso il suddetto sistema), qualora ne ricorrano i presupposti, l'Ufficio RPD provvede a sviluppare la comunicazione all'Autorità Garante ed eventualmente ai soggetti Interessati.

Nello svolgimento di tale compito, i Designati al trattamento possono avvalersi del supporto dei Referenti per la protezione dei dati secondo le seguenti modalità e procedure operative di seguito indicate.

3.3.2 I Referenti protezione dei dati personali

Ai sensi del Regolamento sul modello organizzativo in materia di protezione dei dati personali, D.G.G. n. 35 del 26/2/2021, all'art. 7:
Il Referente protezione dati è nominato dal Dirigente Apicale di struttura, ed è incaricato nella generale attività di supporto al Designato nello svolgimento e nello sviluppo dei compiti di responsabilità al medesimo attribuiti dal Titolare. Nel compimento delle proprie attività il Referente è funzionalmente coordinato dall'Ufficio RPD.

Di seguito viene riportato il dettaglio delle attività previste dal suddetto Regolamento, con riferimento alle procedure supportate dal sistema MUA (Motore Unico Amministrativo).

Individuazione e nomina dei Referenti

I Designati, ciascuno nell'ambito della propria struttura di appartenenza, individuano, tra i dipendenti, i Referenti protezione dei dati personali. L'elenco dei nominativi così prodotto deve essere trasmesso all'Ufficio RPD per l'attivazione della procedura di nomina. Tale "procedura di attivazione digitale" delle nomine prevede:

- caricamento mediante sistema MUA dei soggetti individuati (dall'elenco dei dipendenti, sarà sufficiente "flaggare" i nominativi corrispondenti) da parte dell'Ufficio RPD;
- produzione automatizzata dell'atto di nomina del Referente direttamente dal *software* MUA;
- invio automatizzato (attraverso MUA) al Designato al fine di consentire la sottoscrizione dell'atto da parte dello stesso con firma elettronica avanzata integrata all'interno dello strumento MUA;
- invio automatizzato di una e-mail al Referente al fine di recepire l'atto di nomina già sottoscritto dal Designato;
- attribuzione automatizzata dell'atto di nomina sul sistema MUA per l'archiviazione sulla scheda personale del Referente (e alimentazione della mappatura complessiva dei ruoli *privacy* all'interno dell'Ente).

L'avvio della procedura di gestione automatizzata degli atti di nomina all'interno del sistema MUA verrà comunicata dall'Ufficio RPD ai designati ed ai Referenti. Nelle more dell'avvio della procedura, gli atti di nomina dei referenti potranno essere gestiti attraverso la modulistica analogica già messa a disposizione dall'ufficio RPD e mantenuti agli atti dai Designati al trattamento fino ad ulteriori comunicazioni da parte dell'ufficio RPD.

Attività del Referente relative ai rapporti intercorrenti con soggetti terzi in materia di trattamento e protezione dei dati personali

I Designati individuano i soggetti terzi coinvolti nel trattamento dati correlato a specifiche attività/servizi.

Il Referente della struttura coinvolta – anche nell'ambito delle attività relative all'individuazione di nuovi trattamenti popola il sistema MUA con la descrizione delle caratteristiche del soggetto esterno (mediante una procedura guidata che prevede fattispecie predefinite), laddove non sia già stato precedentemente censito. La procedura automatizzata MUA, a seconda della fattispecie individuata dal Referente, attiva due casi distinti:

1. produzione automatizzata dell'atto di nomina relativo al soggetto esterno (nelle fattispecie previste dall' art. 28 del GDPR) al fine della sottoscrizione e dell'archiviazione nella scheda del soggetto esterno come file allegato;
2. invio di richiesta di parere all'Ufficio RPD attraverso apposito automatismo inserito nel sistema MUA il quale, al verificarsi di determinate circostanze, comunicherà al Referente la necessità di sviluppare una istruttoria da parte dell'RPD, procedendo in autonomia alla comunicazione della casistica all'Ufficio RPD ed all'RPD medesimo, in tale scenario l'Ufficio RPD e l'RPD produrranno manualmente gli atti necessari;

In entrambi i casi l'atto prodotto (in modo automatizzato o dal RPD) viene trasmesso al Referente che si premurerà di farlo sottoscrivere al Designato al trattamento per poi inviare l'atto medesimo al soggetto esterno. Il Referente dovrà periodicamente controllare il re-inoltro dell'atto firmato da parte del soggetto esterno. Una volta ricevuto l'atto sottoscritto, il Referente entrerà nella sezione "enti esterni" del sistema MUA e,

ricercando la scheda dell'ente esterno interessato, allegherà il file dell'atto sottoscritto ricevuto.

▸ Attività del Referente correlate alla gestione del "Registro dei trattamenti": produzione informative *privacy* e gestione dell'analisi del rischio e della valutazione d'impatto

La mappatura dei procedimenti amministrativi/processi dell'Ente e il conseguente popolamento del sistema MUA configura un "Registro dei trattamenti" elaborato a livello centrale, per cui è prevista l'approvazione da parte dei Designati per ciò che riguarda i procedimenti di propria competenza così individuati. Tale versione del Registro dei trattamenti verrà messa a disposizione dei Referenti e dei Designati attraverso il sistema MUA in modo da poter consentire una verifica dei trattamenti medesimi. L'ufficio RPD comunicherà la data di avvio di tale revisione e, se necessarie, eventuali ulteriori istruzioni per agevolare tale verifica.

Nell'ambito di questo "Registro dei trattamenti" tipizzato dall'Ufficio RPD e presente su MUA, il compito del Referente è quello di verificare la completezza dei trattamenti descritti con riferimento alla propria struttura di appartenenza, per eventualmente integrarli (con l'ausilio dell'Ufficio RPD), allo scopo di supportare il processo di approvazione in carico ai Designati.

Nel caso di nuove attività/servizi in capo a ciascuna struttura (che danno luogo a nuovi processi/procedimenti), il Referente ha il compito di attivare la procedura MUA deputata a individuare l'eventuale trattamento dati correlato alla nuova attività; l'attivazione della procedura prevede la compilazione, mediante procedura guidata, di campi specifici relativi alle caratteristiche di natura organizzativa del nuovo progetto. Le specifiche inserite hanno lo scopo di supportare l'istruttoria finalizzata alla definizione del nuovo trattamento, anche in funzione dell'analisi del rischio eventualmente sotteso.

Al fine di definire correttamente le caratteristiche del nuovo trattamento correlato alla nuova attività/servizio, in fase di compilazione del questionario MUA, il referente coinvolto indica la presenza o meno di infrastrutture tecnologiche ovvero applicativi (*asset hardware* e *software*) per la gestione di quell'attività/servizio. Tale segnalazione, se presente, attiva in modo automatizzato il coinvolgimento del DTD, il cui Referente ha il compito di descrivere le caratteristiche tecnologiche nel dettaglio.

Come già indicato, le attività sopra descritte (inserimento a sistema del dettaglio della nuova attività) consentono al sistema MUA di elaborare in modo automatizzato l'analisi dei rischi ed eventualmente richiedere l'inserimento di informazioni aggiuntive per la produzione di una DPIA da parte del Referente. Il livello del rischio così generato viene sottoposto al vaglio del RPD, che:

- procede ad autorizzare il trattamento;
- impone specifiche prescrizioni in caso sia rilevato un livello di rischio elevato.

In caso di approvazione del nuovo trattamento, anche a seguito delle modifiche apportate per l'analisi del rischio, il sistema MUA elabora l'eventuale informativa connessa e il relativo consenso (ove previsto), inviandoli al Referente che ha dato avvio al processo. Il referente dovrà farsi carico di consegnare tale materiale alle strutture di competenza che dovranno integrarlo all'interno delle procedure operative della nuova attività. Il processo, infine, ha come conseguenza l'aggiornamento automatizzato del "Registro dei trattamenti".

La procedura per lo svolgimento delle attività ivi descritte è la medesima di cui al precedente punto 2.2.5.

- ***Compiti del Referente in relazione alla gestione delle richieste degli interessati***

Allo scopo di popolare il "Registro delle richieste degli interessati", le richieste/istanze degli interessati pervenute presso la struttura competente devono essere comunicate al Referente competente per struttura, che deve:

- Registrarla sul sistema MUA mediante questionario guidato (oggetto di specifica formazione) allegando la richiesta pervenuta;

La richiesta così inserita viene presa in carico dall'Ufficio RPD che, sentito il parere del RPD, darà riscontro alla richiesta (anche il parere verrà inserito all'interno del sistema MUA). Sulla base dell'esito di tale istruttoria, il Designato darà riscontro all'interessato.
Qualora l'istanza dovesse essere inviata direttamente all'RPD, l'istruttoria sarà sviluppata dallo stesso dando poi riscontro alla struttura dell'esito della stessa per predisporre poi la risposta agli interessati.

- **Compiti del Referente sulla Gestione "*Data Breach*"**

Come già evidenziato nei paragrafi precedenti, la violazione dei dati personali (o "*Data Breach*") è una 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. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali[1].
Il Titolare del trattamento **senza ingiustificato ritardo** e, ove possibile**, entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche (secondo l'art. 85 del GDPR).

In relazione ai compiti del Referente, la violazione dati può riguardare:

- eventi analogici - ovvero perdite, alterazioni o altre fattispecie di violazione non avvenute su sistemi informatici: in questo caso, l'evento deve essere comunicato da chi ne viene a conoscenza al Referente della struttura in cui è avvenuta la violazione. Il Referente deve inserire tale comunicazione sul sistema MUA, che mediante un questionario guidato, lo supporta nella descrizione delle modalità e delle circostanze dell'incidente. L'attività così condotta consente l'aggiornamento del "Registro *data breach*" fungendo da impulso all'Ufficio RPD che, sentito il parere del RPD, darà riscontro in relazione alla eventuale necessità di successiva comunicazione all'Autorità e agli interessati.
- eventi digitali - ovvero violazioni avvenute su sistemi centralizzati o dei fornitori: quando la violazione avviene su sistemi informativi, il compito di inserire la comunicazione relativa all'avvenuto incidente è del Referente del DTD. Analogamente a quanto accade per gli eventi analogici, l'attività descritta funge da impulso all'Ufficio RPD che, sentito il parere del RPD, darà riscontro alla richiesta sull'eventuale comunicazione al Garante.

[1] https://www.garanteprivacy.it/regolamentoue/databreach

Compiti del Referente in relazione alla nomina degli Autorizzati al trattamento

I Designati individuano, ciascuno nell'ambito della propria struttura di competenza, i dipendenti autorizzati al trattamento dei dati personali.

L'elenco così formato viene trasmesso al Referente, che dà avvio alla "procedura digitale, attraverso il sistema MUA del:

- caricamento dei nominativi (mediante un flag) degli Autorizzati individuati dal Designato;
- produzione automatizzata dell'atto di nomina direttamente dall'applicativo che mediante invio di una e-mail al Designato consente la diretta sottoscrizione dell'atto da parte dello stesso con firma elettronica avanzata;
- comunicazione all'Ufficio RPD dei nominativi degli Autorizzati mediante apposita procedura MUA, allo scopo di aggiornare l'Ufficio sulle nomine effettuate.