Sistema Socio Sanitario

Regione Lombardia

ASST Fatebenefratelli Sacco

REGOLAMENTO SUL MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(approvato con deliberazione del Direttore Generale n. 814 del 06/06/2022)

Capo I – Disposizioni Generali

Capo II - Modello organizzativo

Capo III - Sicurezza e protezione dati

Capo IV – Organizzazione interna

Capo I - Disposizioni generali

Art. 1 Oggetto

Il presente Regolamento sul modello organizzativo in materia di protezione dati personali disciplina l'assetto di *governance* e le disposizioni procedimentali per l'adeguamento dell'ASST (Azienda Socio Sanitaria) Fatebenefratelli Sacco al Regolamento Generale Protezione Dati UE del 27 aprile 2016 n. 679 (RGPD[1]) e al "*Codice in materia di protezione dei dati personali*", D.Lgs. n. 196 del 30 giugno 2003 e s.m.i..

Art. 2 Definizioni

Ai fini del presente Regolamento si intende per:

RGPD: Regolamento Generale Protezione Dati Personali;

Titolare: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

RPD/DPO: Responsabile Protezione Dati Personali/Data Protector Officer;

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 con specifici compiti e funzioni;

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

Interessato: la persona fisica a cui si riferiscono i dati personali;

Autorizzati: è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali;

Data Breach (violazione dei dati personali): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

Art. 3 Presupposti di liceità del trattamento

1. I trattamenti sono effettuati dall'ASST Fatebenefratelli Sacco sulla base dei seguenti presupposti di liceità:

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

- l'esercizio delle funzioni di prevenzione, diagnosi, cura, assistenza sanitaria e socio-sanitaria;
- l'esercizio delle funzioni amministrative direttamente o indirettamente finalizzate alla prevenzione, diagnosi e assistenza sanitaria e socio-sanitaria;
- l'esercizio di ulteriori funzioni amministrative per servizi di competenza affidate dalla legge nazionale o regionale all'ASST Fatebenefratelli Sacco;

[1] Come presente sul sito del Garante

b) adempimento di un obbligo legale al quale è soggetto l'ASST Fatebenefratelli Sacco; la finalità del trattamento è stabilita dalla stessa fonte normativa che lo disciplina;
c) 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.

Capo II - Modello organizzativo

Art. 4 Titolare del trattamento

1. L'ASST Fatebenefratelli Sacco, rappresentata ai fini previsti dal RGPD dal Direttore Generale *pro-tempore*, è il Titolare del trattamento dei dati personali (di seguito, il "Titolare") raccolti anche in banche dati, digitali o cartacee.

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

3. Il Titolare mette in atto le misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati, per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del RGPD e tutte le comunicazioni e informazioni occorrenti per il loro esercizio.

4. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa, di bilancio e di Peg mediante analisi della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'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.

5. Il Titolare provvede a:
a) nominare il Responsabile della protezione dei dati (RPD);
b) nominare i Designati al trattamento dei dati nelle persone del Direttore Amministrativo, del Direttore Sanitario e del Direttore Socio Sanitario, dei Direttori/dirigenti responsabili delle singole UOC/UOSD sanitarie nonché dei Direttori/dirigenti responsabili delle singole UOC/UOSD/UOS dell'area professionale-tecnica-amministrativa (PTA) in cui si articola l'organizzazione, quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti dei dati personali effettuati dall'Ente e preposti al trattamento dei dati contenuti nelle banche dati di competenza delle articolazioni organizzative cui sono preposti;
c) assegnare distinti compiti a specifiche Strutture, in ragione delle peculiari competenze alle medesime attribuite dal Piano Organizzativo Aziendale Strategico (POAS) al fine di avvalersi di particolari contributi ed apporti funzionali per il concreto e fattivo adeguamento dell'Ente al regolamento UE;
d) definire gli indirizzi per l'attribuzione di specifiche competenze all'Ufficio del Privacy Manager, anche con riguardo alla funzione di raccordo e di collaborazione con il Garante per la protezione dei dati personali, al fine di supportare l'attività del Responsabile della protezione dei dati (d'ora in poi "RPD") nel rapporto con le Strutture organizzative dell'Ente e fornire a queste ultime le necessarie indicazioni in materia di protezione dati sui trattamenti sviluppati dalle stesse.

6. Il Titolare è contitolare del trattamento, ai sensi dell'art. 26 del RGPD, nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'ASST Fatebenefratelli Sacco da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento.

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

Art. 5 Responsabile della protezione dati /Data Protector Officer (RDP/DPO)

1. Il Responsabile della protezione dei dati (di seguito, RPD/DPO) è scelto tra il personale dipendente dell'ASST Fatebenefratelli Sacco oppure individuato nella figura unica di un professionista o di una società, nel rispetto delle prescrizioni recate dal Codice degli appalti in materia di contratti di servizio. In entrambi i casi il soggetto deve possedere dei requisiti specificati dagli artt. 37 e 38 del RGPD.

2. Il Responsabile della protezione dei dati è incaricato dei seguenti compiti:
a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati;
b) fungere da supporto alle Strutture competenti sulle richieste di accesso civico generalizzato per tutti gli aspetti relativi alla protezione dei dati personali, ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE 2016/679;
c) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento;
d) rendere una consulenza idonea, scritta od orale, anche nella individuazione dei rapporti intercorrenti con soggetti terzi in materia di protezione dei dati;
e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione;
f) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;
g) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;
h) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del Responsabile della protezione dei dati.

3. La figura del Responsabile della protezione dei dati è incompatibile con chi determina le finalità o i mezzi del trattamento e con il ruolo di fornitore dell'Ente tranne nel caso in cui l'attività di fornitura sia da considerarsi quale ausilio e supporto allo svolgimento delle attività in capo al Responsabile della protezione dei dati medesimo. In particolare, risultano con la stessa incompatibili:
- il Responsabile per la prevenzione della corruzione e per la trasparenza;
- il Responsabile del trattamento;

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

4. Il Responsabile della protezione dei dati dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente. Il Titolare ed il Responsabile del trattamento forniscono al Responsabile della protezione dei dati le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti.
In particolare, al Responsabile della protezione dei dati sono assicurati:
- il supporto attivo per lo svolgimento dei compiti da parte dei Designati di cui all'art. 6 e degli altri organi di natura amministrativa e politica, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa, di bilancio e di Piano della performance;
- le risorse finanziarie, infrastrutturali e di funzionamento (sede, attrezzature, strumentazione) nonché di personale, attraverso la collaborazione dell'Ufficio del Privacy Manager;
- accesso alle articolazioni funzionali dell'Ente per fornire il supporto, le informazioni e gli *input* essenziali.

5. Il Responsabile della protezione dei dati opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti e non deve ricevere istruzioni in merito al loro svolgimento, né sull'interpretazione da dare a una specifica questione riguardante la normativa sulla protezione dei dati personali. Ferma restando l'indipendenza nello svolgimento di detti compiti, il Responsabile della protezione dei dati riferisce direttamente al Titolare od al Responsabile del trattamento. Nel caso in cui siano rilevate dal Responsabile della protezione dei dati o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso Responsabile della protezione dei dati, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art. 6 Designati al trattamento dei dati

1. Il Titolare nomina i Direttori/Dirigenti responsabili delle Strutture in cui si articola l'organizzazione dell'Ente quali Designati al trattamento dei dati personali, relativamente ai trattamenti effettuati dall'articolazione organizzativa di competenza. Ciascun Designato deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità, per mettere in atto, sulla base delle istruzioni fornite dal Titolare, le misure tecniche e organizzative rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

2. Il Titolare, nell'atto di nomina, indica gli specifici ambiti di attività, o l'elenco dei trattamenti di dati personali, cui i singoli Designati sono preposti. Con l'atto di designazione viene formalmente attribuita la delega alla sottoscrizione degli atti contrattuali con i responsabili esterni *ex* art. 28 RGPD legati all'ASST Fatebenefratelli Sacco.

3. Ai Designati sono attribuiti i seguenti compiti:
a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
b) disporre l'attuazione dei provvedimenti emessi dal Garante;
c) collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
d) individuare i soggetti Autorizzati al trattamento per la Struttura organizzativa di competenza e attribuire loro specifici compiti e attività di protezione dei dati;
e) individuare ed incaricare i Referenti Protezione Dati di cui all'art. 6 per la propria Struttura organizzativa;

f) individuare il personale della propria articolazione organizzativa da sottoporre alle attività formative in materia di protezione dei dati;
g) 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;
h) procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza e aggiornare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura organizzativa;
i) individuare e nominare i Responsabili di trattamento e conservare il relativo Registro delle attività;
l) predisporre, in accordo con il RPD, un calendario di audit da svolgere congiuntamente con i Responsabili del trattamento nominati, individuati a campione ovvero a rotazione;
m) adottare, se necessario, specifici disciplinari tecnici di settore, anche congiuntamente con altri Designati e/o Responsabili del trattamento, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla specifica area di competenza;
n) fornire riscontro alle richieste dell'Interessato per i trattamenti di dati di competenza della propria Struttura organizzativa;
o) rilevare e comunicare i casi di violazione dei dati personali, nell'ambito organizzativo di riferimento (*data breach*).

4. Per i trattamenti dei dati personali che coinvolgono più strutture in modo trasversale, laddove applicabile, vige il criterio della prevalenza, secondo il quale la Struttura che ha competenza principale nel trattamento dei dati personali coordina le attività delle altre Strutture coinvolte.

Art. 7 Referenti protezione dati

1. Il Referente protezione dati è nominato dal Direttore/Dirigente responsabile di Struttura, quale Designato al trattamento dati, ed è incaricato della generale attività di supporto al Designato nello svolgimento e sviluppo dei compiti di responsabilità al medesimo attribuiti dal Titolare. Nel compimento delle proprie attività il Referente è funzionalmente coordinato dall'Ufficio del Privacy Manager.

2. I compiti di supporto affidati al Referente riguardano:
a) l'individuazione dei rapporti intercorrenti con soggetti terzi in materia di trattamento e protezione dei dati personali;
b) l'analisi della progettazione delle misure di trattamento dei dati da predisporre preventivamente all'avvio di nuove attività/progetti/servizi;
c) la comunicazione delle modifiche intervenute nei trattamenti di competenza della propria Struttura organizzativa;
d) la gestione delle richieste dell'Interessato per i dati personali trattati dalla Struttura organizzativa preposta;
e) la predisposizione e la proposizione dell'informativa all'Interessato;
f) l'aggiornamento e l'adeguamento dei contenuti della modulistica di competenza della propria Struttura organizzativa alla normativa in materia di protezione dati personali;
g) la formalizzazione e l'aggiornamento degli incarichi agli Autorizzati al trattamento e la verifica e il supporto alla loro attività;
h) adempimenti correlati con la rilevazione dei casi di violazione dei dati personali (*data breach*).

Art. 8 Responsabile del trattamento

1. I soggetti pubblici o privati che trattano dati personali, anche particolari, per conto del Titolare, e che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo che il trattamento soddisfi i requisiti previsti dal Regolamento UE e garantisca la tutela dei dati dell'interessato, assumono il ruolo di Responsabili del trattamento, di cui all'art. 28 del RGPD, mediante atti giuridici in forma scritta, ai sensi dell'art. 6 del presente Regolamento, dei Designati al trattamento dei dati, sulla base di apposita delega del Titolare, per gli ambiti gestionali di propria competenza.

2. I rapporti tra il Titolare ed i Responsabili sono disciplinati dagli atti di cui al comma 1, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del Responsabile del trattamento e le modalità di trattamento. Tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

3. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla normativa e ai compiti affidatigli dal Designato, quale delegato del Titolare.

4. Qualora l'Ente proceda alla nomina di Responsabili dovrà prevedere, in sede di contratto di servizio, che questi ultimi sviluppino il Registro dei trattamenti coordinandosi con l'ASST Fatebenefratelli Sacco.

Art. 9 Autorizzati al trattamento

1. Il Titolare o i Designati, di cui all'art. 6, individuano, nell'ambito di propria responsabilità, gli Autorizzati al trattamento, quali persone ammesse a compiere operazioni sui dati personali.

2. Nell'atto di individuazione, i Designati indicano, per ciascun Autorizzato, gli ambiti di attività e/o l'elenco dei trattamenti di dati personali di competenza.

Art. 10 Ufficio del Privacy Manager aziendale

1. L'Ufficio del Privacy Manager aziendale, anche con l'ausilio di soggetti esterni reclutati con contratto di appalto di servizio, ha il compito di supportare il Responsabile della protezione dei dati personali (RPD) nel rapporto con tutte le Strutture in materia di adeguamento al RGPD. Collabora con il RPD nella definizione della proposta di modello organizzativo in materia di protezione dati personali; si relaziona con le Strutture fornendo linee operative per l'implementazione del medesimo modello prevedendo anche una gestione digitalizzata dei procedimenti, dei processi e delle attività dell'Ente per la corretta e tempestiva applicazione del suddetto Regolamento.

2. All'Ufficio compete l'individuazione di modalità e procedure operative finalizzate alla:
a) trasmissione dei pareri richiesti dalle Strutture organizzative dell'Ente al RPD;
b) individuazione, contrattualizzazione e nomina dei Responsabili di trattamento da parte dei Designati, di cui all'art. 6, comma 3 del presente Regolamento;
c) adozione di soluzioni di privacy *by design e by default;*
d) gestione e conservazione del registro dei trattamenti;
e) gestione dell'analisi del rischio e la valutazione di impatto;
f) gestione *data breach*, violazioni dei trattamenti;
g) coordinamento funzionale dei Referenti per la protezione dei dati;
h)rilevazione del personale individuato dai Designati al trattamento, nell'ambito delle Strutture organizzative dirette, da sottoporre ad attività formativa in materia di protezione dei dati;

i) ricezione e risposta alle richieste degli Interessati inviate direttamente all'Ufficio;
l) presentazione dell'informativa all'Interessato;
m) comunicazione delle modifiche intervenute nei trattamenti di competenza della propria Struttura organizzativa.

Capo III – Sicurezza e protezione dati

Art. 11 Sicurezza del trattamento

1. Il Titolare del trattamento e tutti i soggetti/ruoli descritti al Capo II del presente Regolamento mettono in atto, per i distinti profili di responsabilità e di azione, misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche. Costituiscono misure tecniche ed organizzative che possono essere adottate, tra le altre, i sistemi di autenticazione, autorizzazione, rilevazione di intrusione, sorveglianza; di protezione (antivirus; firewall; antintrusione); 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.

2. La conformità del trattamento dei dati al RGPD è dimostrata attraverso l'adozione delle misure di sicurezza adeguate oppure con l'adesione a codici di condotta approvati ovvero a meccanismi di certificazione approvati.

3. L'ASST Fatebenefratelli Sacco, attraverso i ruoli individuati nel presente Regolamento, si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure anche a coloro che agiscono per suo conto ed abbia accesso a dati personali.

4. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi adottati ai sensi del D. Lgs. 196/2003 nella versione antecedente alle modifiche apportate dal D. Lgs. 101/2018.

Art. 12 Registro del Titolare del trattamento

1. Il Registro delle attività di trattamento svolte dall'Ente reca almeno le seguenti informazioni, come previste dall'art. 30 RGPD:
a) il nome ed i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento e del Responsabile della Protezione 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 od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

3. Il Registro è conservato dall'Ufficio del Privacy Manager per conto del Titolare.

Art. 13 Registro del Responsabile del Trattamento

1. Il Responsabile del trattamento tiene il Registro delle categorie di attività trattate per conto del Titolare contenente:

a) il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile del trattamento, del Rappresentante del Titolare del trattamento o del Responsabile del trattamento e del RPD;
b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il Registro è conservato dal Designato al trattamento, ai sensi dell'art. 6.

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

1 Il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto (DPIA) quando il trattamento medesimo, considerati la natura, l'oggetto, il contesto e le finalità dello stesso nonché l'eventuale utilizzo di nuove tecnologie, presenta un rischio elevato per i diritti e le libertà delle persone fisiche.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti, o non soggetti, a valutazione come redatti e pubblicati dal Garante per la protezione dei dati personali ai sensi dell'art. 35 del RGPD.

3. La DPIA non è necessaria nei casi seguenti:
a) se il trattamento non presenta un rischio elevato per i diritti e le libertà di persone fisiche;
b) 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;
c) se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
d) 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;
e) se i trattamenti sono già stati oggetto di verifica preliminare da parte del Garante della Privacy o del RPD e che proseguono con le stesse modalità oggetto di tale verifica.

Art. 15 Violazione dei dati personali

1. 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 non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ente.

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

3. 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. Se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto. Il

Titolare del trattamento, a prescindere dalla notifica al Garante, documenta tutte le violazioni dei dati personali, secondo le modalità individuate dall'Ufficio Privacy. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

4. Il Responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il Titolare in modo che possa attivarsi.

5. Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Capo IV – Organizzazione interna

Art. 16 Struttura competente in materia di comunicazione e di *governance* dei servizi offerti alla cittadinanza

1. La struttura competente in materia di comunicazione istituzionale e di governance dei servizi offerti all'utenza fornisce il contributo nella definizione dei processi e/o requisiti funzionali dei servizi digitali relativamente all'impatto di questi sulle attività di trattamento, fatte salve le eventuali specifiche competenze attribuite alla medesima struttura dal Titolare.

2. La struttura, in particolare, svolge i seguenti compiti di coordinamento e supporto alle articolazioni organizzative dell'Ente:
a) aggiornamento dei contenuti e delle informative presenti sul portale istituzionale, al fine di favorire l'omogenea applicazione delle disposizioni in materia di protezione dei dati;
b) definizione dei processi e/o requisiti funzionali dei servizi digitali inerenti l'analisi del rischio (ai sensi dell'art. 32 del RGDP) e della valutazione d'impatto (ai sensi dell'art. 35 del RGDP) attraverso criteri e modelli concordati con l'Ufficio del Privacy Manager.

Art 17 Struttura competente in materia di transizione digitale

1. La Struttura competente in materia di transizione digitale che opera in supporto al Responsabile per la Transizione al Digitale (RTD) individuato nell'ente ai sensi dell'art.17 del CAD (Codice Amministrazione Digitale), in ambito di protezione dati, fornisce il contributo nella valutazione degli aspetti tecnologici relativamente all'impatto di questi sulle attività di trattamento, fatte salve le eventuali specifiche competenze attribuite alla medesima struttura dal Titolare.

2. La struttura, in particolare, svolge i seguenti compiti:
a) realizzazione di una apposita base di dati contenente le caratteristiche dell'infrastruttura tecnologica *hardware* e *software* utilizzata dall'Ente per le attività di trattamento di dati, secondo modalità sviluppate di comune accordo con l'Ufficio Privacy e con RTD;
b) sviluppo degli aspetti tecnologici inerenti l'analisi del rischio (ai sensi dell'art. 32 RGPD) e della valutazione di impatto (ai sensi dell'art. 35 RGPD) attraverso criteri e modelli concordati con l'Ufficio del Privacy Manager e con il RTD;
c) supporto alle Strutture organizzative nel caso di istanze degli Interessati che richiedano valutazioni di natura tecnologica relative agli strumenti di trattamento dati utilizzati dal Titolare;
e) predisposizione della procedura interna di segnalazione *data breach,* secondo modalità sviluppate di comune accordo con l'Ufficio del Privacy Manager e parere del RDP/DPO, nel caso di una violazione che abbia avuto ad oggetto sistemi tecnologici del Titolare del Trattamento o dei Responsabili del Trattamento nel rispetto di quanto previsto all'art. 15 del presente Regolamento.

Art. 18 Rinvio

1. Per tutto quanto non espressamente disciplinato, si applicano le disposizioni del RGPD e tutte le norme vigenti in materia.