CASA DI RIPOSO
CARTIGLIANO

PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO A TUTELA DEI DATI PERSONALI

approvato con deliberazione del C.d.A. n. 18 del 18/09/2020

CASA DI RIPOSO CARTIGLIANO

RGDP = Regolamento Generale sulla Protezione dei Dati Personali, Regolamento UE n. 679/2016.

RPD = Responsabile della Protezione dei dati (in inglese **DPO** Data Protection Officer).

Data breach = "Riuscire a fare breccia", qualunque violazione dei dati personali.

DPIA = Valutazione di impatto sulla protezione dei dati.

Privacy by design = Privacy dal momento della sua progettazione. Implica che qualsiasi progetto va realizzato assumendo dalla fase iniziale di ideazione misure di protezione di dati personali.

Privacy by default = Protezione dei dati per impostazione predefinita, ovvero, misure tecniche ed organizzative che assicurano solo i dati personali necessari per ogni specifica finalità di trattamento.

Audit Privacy = Valutazione dei processi interni adottati sul grado di rispetto della normativa vigente del Reg. UE n. 679/2016.

GEPD = Garante Europeo della protezione dei dati.

Accountability = Letteralmente "rendere conto", ovvero, il Titolare del trattamento si deve responsabilizzare autonomamente nella gestione ed organizzazione della Privacy. Il principio nasce nella legislazione europea e statunitense ed è inteso come la responsabilità dell'amministrazione ha verso chi l'ha scelta e si fonda su: trasparenza intesa come informazioni dell'attività di governo; partecipazione di chiunque al miglioramento delle politiche pubbliche e collaborazione intesa come efficacia dell'azione amministrativa attraverso la cooperazione tra tutti i livelli di governo.

WP 29 = Warking Party Art. 29 (c.d. Gruppo di lavoro art. 29). Organismo consultivo ed indipendente composto da un rappresentante dei Garanti dei dati personali di ogni stato membro, da un rappresentante della Commissione UE e dal Garante europeo della protezione dei dati.

PREMESSA

Il 25 maggio 2018 è divenuto ufficialmente operativo il nuovo Regolamento generale in materia di Protezione dei Dati personali.
Il GDPR, acronimo di "General Data Protection Regulation" va ad abrogare, dopo oltre un ventennio, la cosiddetta direttiva madre n. 95/46/C che, fino ad oggi, costituiva il quadro normativo di riferimento a livello europeo.
Il nuovo Regolamento costituisce, insieme alla Direttiva (UE) n. 2016/680, il "Pacchetto di protezione dei dati" elaborato ed approvato dall'Unione Europea.
Il Reg. (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 fa riferimento a dati concernenti persone identificate o identificabili in possesso di vari soggetti e quindi anche della Pubblica amministrazione utilizzabili per le proprie finalità istituzionali. Dati che devono essere trattati nei limiti delle funzioni dell'ente, il quale avrà anche l'obbligo di proteggerli con nuovi strumenti.
Il nuovo apparato normativo si regge su di un nuovo principio di fondamentale importanza: la responsabilizzazione, ovvero il principio di accountability (nell'accezione inglese). Tale concetto rappresenta un'assoluta novità nel campo della protezione dei dati personali, in quanto il titolare del trattamento, oltre ad avere l'esclusiva competenza per il rispetto dei principi e delle regole previste dal GDPR, deve anche essere in grado di comprovarne il corretto adempimento.
Ai titolari, altresì, viene affidato il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri indicati dal regolamento.
Come specifica chiaramente l'art. 25 del GDPR, uno di quei criteri è sicuramente rappresentato dall'espressione anglofona "*data protection by default and by design*", ossia dalla necessità di configurare il trattamento prevedendo dall'inizio, ovvero fin dalla fase di progettazione, le garanzie indispensabili "*al fine di soddisfare i requisiti*" del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
Spetta dunque al titolare mettere in atto una serie di misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento.
Tra le nuove attività previste dal GDPR, riguardo agli obblighi dei titolari, saranno fondamentali quelle relative alla valutazione del rischio inerente il trattamento. Quest'ultimo è da intendersi come rischio da impatti negativi sulle libertà e sui diritti degli interessati; tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione, tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per diminuirne l'impatto.
Una lettura organica e sistematica del Regolamento europeo consente di affermare che, data l'importanza della normativa e di ciò che essa mira a proteggere, la migliore risposta in termini di cambiamento organizzativo sia quella di realizzare un complessivo "**Modello organizzativo e di gestione**" per la protezione dei dati personali, considerando come tale un complesso di attività organizzativa, di ruoli, di azioni organizzative, di sistemi mirato al fine dell'applicazione "ordinata" e completa, nell'azione amministrativa dell'Ente, della normativa sui trattamenti di dati personali. Tale logica di costruzione di un Modello ad hoc è, peraltro, simile a quella risultante, in materia di prevenzione della corruzione.
L'adeguamento al Regolamento UE 2016/679 impone al Titolare di trattamento pubblico di prestare grande attenzione al fattore organizzativo. Per questo, il Modello organizzativo individua le politiche, gli obiettivi strategici e gli standard di sicurezza per garantire la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati personali, definendo il quadro delle misure di sicurezza informatiche, logiche, logistiche, fisiche, organizzative e procedurali da adottare e da applicare per attenuare e, ove possibile, eliminare il rischio di violazione dei dati derivante dal trattamento.

Al fine di garantire la migliore e più puntuale attuazione del principio di accountability, il presente modello organizzativo contiene disposizioni regolamentari minime la cui concreta attuazione è demandata all'organizzazione del personale operante all'interno dell'ente, nelle sue articolazioni gerarchiche. E' ammesso ed anzi incoraggiato l'utilizzo di modulistica differente rispetto a quella allegata al presente modello a condizione che essa ne rispetti i criteri e le regole generali. Il presente modello organizzativo sarà sottoposto a revisione ogni qualvolta si renderà necessario e, comunque, a cadenza almeno annuale.

PARTE I - NORME E PRINCIPI GENERALI

Questa Amministrazione assicura che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.

In attuazione del suddetto principio l'ente assicura che, nello svolgimento dei compiti e funzioni istituzionali, i dati personali siano trattati nel rispetto della legislazione vigente oltre che dei seguenti principi:

a. «liceità, correttezza e trasparenza»: i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b. «limitazione delle finalità»: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'art. 89, prf. 1 del RGDP, considerato incompatibile con le finalità iniziali;
c. «minimizzazione dei dati»: i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d. «necessità»: è ridotta al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità possano essere perseguite mediante dati anonimi o con l'uso di opportune modalità che permettono di identificare l'interessato solo un caso di necessità;
e. «esattezza»: i dati personali sono esatti e, se necessario, aggiornati; sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
f. «limitazione della conservazione»: i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89, prf. 1 del GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste a tutela dei diritti e delle libertà dell'interessato;
g. «integrità e riservatezza»: i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
h. «responsabilizzazione»: il titolare del trattamento è competente per il rispetto dei principi di cui al comma 1 e deve essere in grado di comprovarlo.

Sensibilizzazione e formazione

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle pubbliche amministrazioni, di una riservatezza totale dal punto di vista reale e sostanziale.

Ai fini della corretta e puntuale applicazione della disciplina relativa ai principi, alla liceità del trattamento, al consenso, all'informativa e, più in generale, alla protezione dei dati personali, l'ente sostiene e promuove, all'interno della propria struttura organizzativa, ogni strumento di sensibilizzazione che possa consolidare la consapevolezza del valore della riservatezza dei dati, e migliorare la qualità del servizio. A tale riguardo, questa Amministrazione riconosce che uno degli strumenti essenziali di sensibilizzazione sia rappresentato dall'attività formativa del personale nonché quella diretta a tutti coloro che hanno rapporti con l'ente.

Per garantire la conoscenza capillare delle disposizioni normative vigenti, al momento dell'ingresso in servizio, è data ad ogni dipendente una specifica comunicazione, con apposita clausola inserita nel contratto di lavoro, contenente il richiamo ai principi ed alle norme di cui al presente Modello organizzativo, oltre che alle vigenti disposizioni nazionali e comunitarie.

L'ente organizza, nell'ambito della formazione continua e obbligatoria del personale, specifici interventi di formazione e di aggiornamento in materia di protezione dei dati personali, finalizzati alla conoscenza delle norme, alla prevenzione di fenomeni di abuso e illegalità nell'attuazione della normativa, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni agli interessati.

La formazione in materia di prevenzione dei rischi di violazione dei dati personali viene integrata e coordinata con la formazione in materia di trasparenza e di accesso, con particolare riguardo ai rapporti tra protezione dei dati personali, trasparenza accesso ai documenti amministrativi e accesso civico, semplice e generalizzato, nei diversi ambiti in cui opera l'ente.

La partecipazione dei dipendenti agli interventi formativi viene considerata quale elemento di misurazione e valutazione della performance organizzativa ed individuale.

Trattamento dei dati personali

L'ente tratta i dati personali necessari per lo svolgimento delle proprie finalità istituzionali, quali identificate da disposizioni di legge, statutarie e regolamentari, e nel rispetto dei limiti imposti dalla vigente normativa in materia di protezione dei dati personali e dai provvedimenti delle Autorità di controllo.

Le operazioni di trattamento possono avvenire esclusivamente ad opera dei soggetti all'uopo delegati, designati ed autorizzati secondo quanto previsto nel presente documento.

Non è consentito il trattamento da parte di persone non puntualmente autorizzate ed istruite in tal senso.

Al fine di garantire la correttezza delle operazioni di trattamento l'ente provvede alla ricognizione di tutti i trattamenti di dati personali effettuati nell'ambito dei processi e procedimenti svolti, finalizzata alla compilazione ed aggiornamento del Registro delle attività di trattamento di cui al GDPR.

Tipologie di dati trattamenti

Nell'ambito delle operazioni di trattamento conseguenti all'esercizio delle proprie funzioni istituzionali l'ente tratta in modo anche automatizzato, totalmente o parzialmente, le seguenti tipologie di dati:

- dati personali, quali definiti all'articolo 4, paragrafo 1 del GDPR;
- categorie particolari di dati personali di cui all'articolo 9, paragrafo 1 del GDPR (c.d. dati sensibili);
- categorie particolari di dati personali di cui all'articolo 2-septies del D.Lgs. 196/2003 (c.d. dati super-sensibili);
- dati personali relativi a condanne penali e reati di cui all'articolo 10 del GDPR (c.d. dati giudiziari)

Finalità del trattamento

L'ente effettua periodicamente una ricognizione delle finalità che impongono o consentono il trattamento dei dati personali, anche sensibili (e super-sensibili) e giudiziari.

Circolazione dei dati personali

Fatto salvo il rispetto di specifiche e puntuali disposizioni, l'ente favorisce la circolazione all'interno dei propri uffici dei dati personali dei cittadini il cui trattamento sia necessario ai sensi degli articoli 6, 9 e 10 del GDPR. La circolazione, ove possibile, è assicurata mediante l'accessibilità diretta delle banche dati informative detenute da ciascun ufficio, previa creazione di appositi profili di utenza che tengano conto dei profili di autorizzazione conferiti. Forme similari di accessibilità sono garantite in favore di contitolari e responsabili del trattamento, limitatamente ai dati personali diversi da quelli contemplati dagli articoli 9 e 10 del GDPR.

Coordinamento di norme

Questa Amministrazione intende perseguire l'obiettivo di assicurare le forme più estese di accessibilità e trasparenza sul proprio operato ad opera dei cittadini, nelle varie forme in cui il diritto di accesso è riconosciuto, quali (a titolo esemplificativo) quella prevista dalla Legge 241/90 e quella prevista dal D.Lgs. 33/2013. A tale proposito - fermo restando che i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso ai documenti amministrativi e del diritto di accesso civico, semplice e generalizzato e la relativa tutela giurisdizionale, così come gli obblighi di pubblicità e pubblicazione restano disciplinati dalla normativa di settore - gli uffici dovranno interpretare la vigente normativa in materia di trasparenza ed accesso in modo da garantire la più rigorosa tutela dei dati personali degli interessati, anche tenendo in considerazione le motivazioni addotte dal soggetto (eventualmente, in caso di accesso) controinteressato.

In attuazione dei principi contenuti nella normativa nazionale e comunitaria vigente, l'ufficio, nel dare riscontro alle richieste di accesso ovvero nel pubblicare i provvedimenti, dovrebbe in linea generale scegliere le modalità meno pregiudizievoli per i diritti dell'interessato, privilegiando l'ostensione di documenti con l'omissione dei «dati personali» in esso presenti, laddove l'esigenza informativa, alla base dell'accesso o della trasparenza e pubblicazione, possa essere raggiunta senza implicare il trattamento dei dati personali.

PARTE II - PROFILO ORGANIZZATIVO

Profilo strutturale

La prima risposta organizzativa è l'individuazione di una struttura organizzativa per la protezione dei dati personali, che, ovviamente, si sovrapponga, in gran parte, all'attuale struttura amministrativa dell'ente, integrandosi con essa.

La creazione di tale struttura, comporta tre azioni principali:

- il disegno di struttura (organigramma) per la Privacy;
- la definizione dei ruoli;
- l'individuazione dei soggetti "abilitati" dall'ente a trattare i dati personali.

Conseguente, alla costruzione, sarà quindi necessario adeguare le competenze mediante la formazione e informazione dei soggetti, abilitando concretamente i soggetti stessi.

Il Titolare del trattamento

L'art. 4 n. 7 del GDPR precisa che il titolare del trattamento (interpretando la norma rispetto all'ente locale) è "*l'autorità pubblica*" che "*determina le finalità e i mezzi del trattamento di dati personali*". Il concetto di Titolare del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati.

Competenze e responsabilità

Le competenze e le responsabilità che il GDPR assegna al Titolare del trattamento possono così essere riassunte:

a. determinare le finalità ed i mezzi del trattamento dei dati personali: in considerazione del carattere pubblico che contraddistingue questa Amministrazione, le finalità sono determinate e circoscritte in quelle necessarie a garantire il corretto svolgimento delle funzioni istituzionali e dei compiti di interesse pubblico (art. 4);
b. mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR (c.d. accountability) (art. 24);
c. garantire che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali non tratti tali dati se non è adeguatamente istruito in tal senso (artt. 29 e 32);
d. individuare i responsabili del trattamento, controllarne e garantirne l'operato (art. 28);
e. agevolare l'esercizio dei diritti dell'interessato (art. 12) e fornire agli interessati le informazioni previste dal GDPR (art. 13);
f. designare il Responsabile della protezione dei dati (art. 37) ponendolo in grado di svolgere adeguatamente l'attività (art. 38);
g. istituire e tenere aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
h. effettuare, prima di procedere al trattamento, una valutazione dell'impatto sulla protezione dei dati personali (art. 35);
i. comunicare all'autorità di controllo (art. 33) ed all'interessato (art. 34) eventuali violazioni dei dati;
j. ricevere ed osservare provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
k. rispondere per il danno cagionato dal trattamento che violi il GDPR (art. 82);
l. rispondere delle violazioni amministrative ai sensi del GDPR (art. 83).

Alla luce del testo normativo e delle interpretazioni correnti, si ritiene che titolare sia l'ente locale nel suo complesso in quanto la legislazione nazionale gli ha affidato il compito di raccogliere e trattare certi dati personali. Le competenze e le responsabilità quali delineate dal GDPR e dalla normativa nazionale in tema di protezione dei dati personali sono attribuite agli organi dell'ente in relazione alle funzioni agli stessi assegnati dallo statuto dell'Ente. Tale ripartizione è così intesa da questa Amministrazione:

A. al C.d.A. sono assegnate eventuali competenze di tipo regolatorio o programmatorio generale in materia di riservatezza dei dati;
B. all'organo esecutivo (Dirigente) sono assegnate tutte le competenze a carattere non gestionale e non rientranti nella competenza del Consiglio, con particolare riferimento agli atti e attività a contenuto organizzativo e di indirizzo;
C. all'organo di vertice spettano i seguenti compiti:
    a. le nomine e le designazioni rilevanti in materia di protezione dei dati personali, con riferimento in particolare al Responsabile della protezione dei dati, ai soggetti designati con funzioni di coordinamento, Dirigenti e Responsabili di posizione organizzativa;
    b. verificare la legittimità dei trattamenti di dati personali effettuati dall'ente;
    c. disporre, in conseguenza alla verifica di cui alla lett. b) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
    d. aggiornare costantemente il registro delle attività di trattamento;
    e. garantire la corretta informazione e l'esercizio dei diritti degli interessati;
    f. disporre l'adozione dei provvedimenti imposti dal Garante;
    g. collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
    h. la preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche e le eventuali consultazioni con il Garante ai sensi dell'art. 36 del Regolamento;
    i. gestire la procedura in relazione alle violazioni di dati personali, curando la notifica all'Autorità di controllo e l'eventuale comunicazione agli interessati;
    j. individuare i contitolari del trattamento fornendo le necessarie indicazioni;
D. ai Dirigenti e Responsabili di posizione organizzativa, secondo l'ambito di competenza, spettano i seguenti compiti (con elencazione meramente esemplificativa):
    a. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
    b. disporre, in conseguenza alla verifica di cui alla lett. a) le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
    c. adottare soluzioni di privacy by design e by default;
    d. contribuire al costante aggiornamento del registro delle attività di trattamento;
    e. garantire la corretta informazione e l'esercizio dei diritti degli interessati;
    f. individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche "autorizzati") fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite;
    g. coadiuvare il Titolare nell'adozione dei provvedimenti imposti dal Garante;
    h. collaborare con il Responsabile della protezione dei dati personali al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;

i. garantire al Responsabile della protezione dei dati personali ed al personale (eventualmente) designato Amministratore di sistema i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
j. assistere il Titolare nella preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
k. coadiuvare il Titolare nel gestire la procedura in relazione alle violazioni di dati personali;
l. individuare i responsabili (esterni) e i contitolari del trattamento, fornendo le necessarie indicazioni.

L'autorizzato al trattamento

Il GDPR non prevede espressamente la figura degli "incaricati" e, tuttavia, tale figura può essere implicitamente desunta dall'articolo 29, rubricato "Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento", il quale stabilisce che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*". Il Codice privacy, all'articolo 2-quaterdecies prevede che "*Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".

Il GDPR e la normativa nazionale di adeguamento, consentono dunque di mantenere le funzioni ed i compiti assegnati a figure interne all'ente che, ai sensi del Codice nel testo previgente all'adeguamento al GDPR, ma non anche ai sensi del GDPR, potevano essere definiti come "incaricati". Il personale operante (a qualunque titolo ed a qualunque livello) all'interno dell'Ente è conseguentemente autorizzato al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione redatto in conformità al presente modello organizzativo.

La designazione delle persone fisiche autorizzate al trattamento e l'attribuzione dei compiti e delle funzioni inerenti discendono da (elencazione meramente esemplificativa):

- Statuto dell'ente;
- regolamento di organizzazione degli uffici;
- dotazione organica;
- deliberazioni di approvazione del bilancio.;
- atti di nomina Responsabili di Posizione Organizzativa;
- atti di nomina a Responsabili di Procedimento.

Spetta sia al Titolare sia ai Dirigenti / Responsabili di P.O. impartire analitiche istruzioni e controllare costantemente che le persone fisiche designate, delegate e autorizzate al trattamento dei dati effettuino le operazioni di trattamento:

- in attuazione del principio di «liceità, correttezza e trasparenza»;
- in attuazione del principio di «minimizzazione dei dati»;
- in attuazione del principio di «limitazione della finalità»;
- in attuazione del principio di «esattezza»;
- in attuazione del principio di «limitazione della conservazione»;

- in attuazione del principio di «integrità e riservatezza»;
- in attuazione del principio di «liceità, correttezza e trasparenza».

Dirigenti / Responsabili di Posizione Organizzativa (P.O.) - Designati al trattamento

L'articolo 28 del GDPR ha definito il Responsabile del trattamento come il soggetto che effettua il trattamento "*per conto del titolare*". In forza del rapporto di immedesimazione organica che intercorre tra i Dirigenti / Responsabili di Posizione organizzativa (P.O.) ed il Titolare, non risulta configurabile un rapporto di rappresentanza "*per conto del titolare*".

Conformemente alle disposizioni del GDPR e del Codice della privacy nel suo testo vigente, il Titolare ed i Responsabili di P.O. possono designare, sotto la propria responsabilità ed all'interno del proprio assetto organizzativo, determinate persone fisiche per attribuire alle stesse specifici compiti e funzioni connessi al trattamento dei dati, individuando le modalità più opportune per autorizzare dette persone al trattamento dei dati.

Questa Amministrazione ritiene dunque che i Dirigenti / Responsabili di Posizione organizzativa (P.O.) debbano conseguentemente essere autorizzati al compimento delle operazioni di trattamento dei dati necessarie allo svolgimento delle mansioni e funzioni assegnate, sulla base di uno specifico atto di designazione (di nomina del Titolare al Responsabile di Posizione Organizzativa).

Considerato che ai Dirigenti (e ai Responsabili di P.O.) spetta l'adozione degli atti e provvedimenti amministrativi, compresi tutti gli atti che impegnano l'amministrazione verso l'esterno, nonché la gestione finanziaria, tecnica ed amministrativa mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo e che essi sono responsabili, in via esclusiva, dell'attività amministrativa, della gestione e dei risultati della struttura organizzativa a cui sono preposti, appare opportuno attribuire loro specifici compiti e funzioni spettanti al Titolare, ferma restando l'imputazione della responsabilità conseguente al trattamento in capo al Titolare medesimo. Oltre ai compiti indicati nella Parte II del presente documento, sezione "IL TITOLARE DEL TRATTAMENTO" > "Competenze e responsabilità", il Titolare, con proprio atto, può attribuire ulteriori specifici compiti e funzioni ai Dirigenti / Responsabili di posizione organizzativa (P.O.).

Il referente del responsabile per la protezione dei dati personali

Ai sensi dell'articolo 38 del GDPR, il Titolare ha l'obbligo di assicurarsi che "*il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*"; il Titolare inoltre sostiene "*il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*".

Si ravvisa dunque la necessità - nell'ottica di un adeguamento in qualità ai nuovi istituti previsti dal GDPR, alla luce del contesto, della natura e della complessità dei trattamenti effettuati - di individuare uno o più dipendenti interni all'ente cui assegnare il compito di "Referente" al fine di supportare l'attività del Responsabile della Protezione dei dati personali (RPD o DPO), nelle seguenti attività:

a) Informazione e consulenza al Titolare del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR. Tale attività comporta il supporto nella redazione di pareri, note, circolari, policy, newsletter con segnalazione delle novità normative e giurisprudenziali in materia di protezione dei dati personali e delle migliori best practice in materia di analisi e valutazione dei rischi.

b) Sorveglianza dell'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.
c) Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR. Tale attività comporta un supporto nelle interviste a responsabili di settore, ICT, partecipazione a riunioni, analisi di documentazione tecnica, studio degli ambienti di prova dei software e della relativa documentazione tecnica.
d) Cooperare con l'Autorità di controllo e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva prevista dall'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione. Tale attività comporta un supporto nel riscontro alle richieste di informazioni inviate dal Garante e nelle eventuali ispezioni dell'Autorità.

Il Referente è tenuto al segreto od alla riservatezza in merito all'adempimento dei propri compiti e alle informazioni e dati di cui potrebbe venire a conoscenza nell'esercizio delle proprie funzioni. Egli è inoltre tenuto a segnalare al RPD ogni possibile situazione di conflitto di interesse, anche potenziale rispetto ai propri compiti, incarichi e funzioni.

Ove i compiti assegnati al Referente vengano svolti in modo collettivo da parte di un team, dovrà essere designato un soggetto coordinatore.

Spetta al Titolare identificare e designare il Referente.

Amministratore del sistema informatico

Al fine di ottemperare a quanto disposto dal Garante della Privacy con il provvedimento datato 27/11/2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" come modificato con successivo provvedimento datato 25/06/2009, l'ente si avvale di un amministratore del sistema informatico a garanzia che il sistema informatico di questo Ente sia strutturato e gestito in modo da consentire l'attuazione delle misure tecniche e organizzative adeguate per la necessaria protezione dei dati personali trattati attraverso lo stesso sistema.

L'amministratore del sistema deve essere in possesso di comprovate conoscenze specialistiche tecniche e giuridiche in materia di sicurezza degli strumenti e dei programmi informatici per la protezione dei dati personali nonché della capacità di assolvere i compiti di competenza. Amministratore del sistema informatico può essere designato un dipendente a tempo indeterminato inquadrato almeno nella categoria "C" ovvero, nel caso di mancanza di un dipendente, un soggetto esterno.

Nell'atto o nel contratto di servizio con cui è designato l'Amministratore di sistema devono essere riportati, altresì, tutti gli adempimenti - con tutto ciò che essi comportano sia sul piano delle procedure amministrative, che dell'organizzazione, che dell'adozione e verifica di ogni misura necessaria in materia di protezione dei dati personali - imposti dalle fonti di diritto europee e nazionali, dal "Gruppo di Lavoro europeo ex art. 29", dal Garante della Privacy, dalle disposizioni regolamentari e dalle direttive emanate dal Titolare del trattamento e dal Responsabile della protezione dei dati, nonché per conformarsi alla disciplina del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82/2004 e ss.mm.ii., in particolare la cura dei seguenti adempimenti:

a. gestire l'hardware e i software dei server e delle postazioni di lavoro informatizzate;
b. impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;

c. registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte degli amministratori di sistema; impostare e gestire un sistema di autorizzazione per i componenti degli organi di governo e di controllo interno, per il Responsabile per la protezione dei dati, per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici nonché di quanti siano autorizzati all'accesso ai dati personali contenuti nelle banche-dati informatizzate;
d. verificare costantemente che l'ente abbia adottato le misure tecniche e organizzative adeguate per la sicurezza dei dati personali, provvedendo a proporre adeguamenti eventualmente necessari;
e. suggerire all'Ente l'adozione e l'aggiornamento delle misure di sicurezza adeguate per assicurare la sicurezza dei dati, atte a che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

All'Amministratore del sistema informatico è:

a) fatto assoluto divieto di leggere, copiare, stampare o visualizzare i documenti o i dati degli utenti memorizzati sul sistema a meno che questo sia strettamente indispensabile per le operazioni attinenti ai ruoli allo stesso assegnati; tale divieto vale anche nei confronti di quanti non siano stati autorizzati dal Titolare o dai Responsabili del trattamento a conoscere i dati personali oggetto di trattamento;
b) obbligato a dare tempestiva comunicazione al Titolare nonché al Responsabile della protezione dei dati dei problemi di affidabilità sia dell'hardware che dei software eventualmente rilevati;
c) obbligato a osservare scrupolosamente le informazioni e le disposizioni allo stesso impartite in merito alla protezione dei sistemi informatici, degli elaboratori e dei dati, sia da intrusioni che da eventi accidentali, il trattamento consentito, l'accesso e la trasmissione dei dati, in conformità ai fini della raccolta dei dati.

Il Responsabile della protezione dei dati procederà periodicamente alla verifica delle attività svolte dall'Amministratore del sistema informatico in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Il Contitolare del trattamento (ove previsto)

In base alla previsione contenuta nell'articolo 26 del GDPR "*Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati*".

In coerenza con la propria missione e i propri valori, i Contitolari si impegnano reciprocamente a proteggere i dati personali di ogni persona fisica che si trovasse ad avere contatto o ad operare con i medesimi ("Interessato"), nel rispetto dell'identità, della dignità di ogni essere umano e delle libertà fondamentali costituzionalmente garantite nel rispetto del GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione degli stessi.

Spetta sia al Titolare sia ai Dirigenti e Responsabili di posizione organizzativa, per la struttura organizzativa di competenza, identificare gli eventuali contitolari di riferimento e sottoscrivere gli accordi per il trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai contitolari

l'elenco nominativo delle persone fisiche che, presso gli stessi contitolari, risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni.

Ciascuno dei Contitolari identifica un referente interno alla propria struttura, con il compito di relazionarsi con analogo soggetto designato dall'altra parte, a presidio del corretto adempimento di quanto previsto dal presente accordo. Il nominativo ed i dati di contatto del referente interno sono tempestivamente comunicati all'altra parte. I Contitolari designano congiuntamente un referente unitario quale punto di contatto per gli interessati. Le richieste di esercizio dei diritti e gli eventuali reclami presentati dagli interessati saranno gestiti in via esclusiva dal referente unico, contattabile ai recapiti che saranno resi noti unitamente al suo nominativo, restando in ogni caso inteso che gli interessati potranno esercitare i propri diritti nei confronti di ciascun Contitolare.

I Contitolari si obbligano, in solido tra loro, a predisporre, attuare e mantenere aggiornati tutti gli adempimenti previsti in materia di protezione dei dati personali. E' tuttavia ammessa una diversa ripartizione "Interna" del profilo di responsabilità, da valutarsi caso per caso.

Il responsabile del trattamento (esterno all'organizzazione)

Il concetto di "Responsabile del trattamento" riveste un ruolo importante nel contesto della riservatezza e sicurezza dei trattamenti poiché serve ad individuare le responsabilità di coloro che si occupano più da vicino dell'elaborazione dei dati personali, sotto l'autorità diretta del Titolare del trattamento o per suo conto.

L'esistenza di un Responsabile del trattamento dipende da una decisione presa dal Titolare. Quest'ultimo può decidere di trattare i dati all'interno della propria organizzazione - ad esempio attraverso collaboratori autorizzati a trattare i dati sotto la sua diretta autorità - o di delegare tutte o una parte delle attività di trattamento a un'organizzazione esterna.

A norma dell'articolo 28, paragrafo 1 del GDPR "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*".

Per poter agire come Responsabile del trattamento occorrono quindi due requisiti: essere una persona giuridica distinta dal Titolare ed elaborare i dati personali per conto di quest'ultimo. La liceità dell'attività di trattamento dei dati da parte del Responsabile è determinata dal mandato ricevuto dal Titolare del trattamento. Se va al di là del proprio mandato e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, il Responsabile diventa (con)Titolare. Si deve tuttavia prendere atto del fatto che esistano situazioni in cui la relazione tra l'Amministrazione ed un altro soggetto, pubblico o privato, possa generare dei dubbi in merito alla corretta qualificazione del ruolo soggettivo rivestito (Titolare o Responsabile). Con riferimento a tali fattispecie, questo ente adotta il criterio della valutazione delle circostanze di fatto, suggerito dal Gruppo ex art. 29 nel Parere 1-2010 (WP 169). Il paragrafo 3 dell'articolo 28 del GDPR prevede che "*I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*"; il paragrafo 9, da ultimo, prevede che "*Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico*".

Spetta ai Dirigenti / Responsabili di P.O. identificare i responsabili e gli eventuali sub responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere i contratti/appendici contrattuali per il trattamento dei dati, avendo cura di tenere costantemente aggiornata la relativa documentazione nonché acquisire dai responsabili e dagli eventuali sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi, risultano autorizzate al trattamento dei dati ed a compiere le relative operazioni. Il Dirigente / Responsabile di P.O.

competente per materia in relazione al compito e/o al servizio affidato ha il dovere di verificare che il soggetto esterno osservi le predette prescrizioni; l'Amministratore del sistema informatico verifica che siano osservate le norme riferite all'attuazione delle misure minime di sicurezza. La periodicità delle predette verifiche, previste nel provvedimento o contratto di affidamento, è determinata in funzione della natura dei dati, della probabile gravità dei rischi, dei mezzi da utilizzare per il trattamento e della durata dell'affidamento. Le verifiche e i risultati delle stesse sono registrate in appositi distinti verbali, sottoscritti, in duplice originale, dal Responsabile del trattamento e dal soggetto che svolge ciascuna verifica.

Il responsabile della protezione dei dati personali (RPD o DPO)

L'ente si avvale obbligatoriamente di un Responsabile della protezione dei dati (RPD o DPO), in possesso delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di competenza.

Il Responsabile della protezione è designato con atto del Titolare.

Responsabile della protezione dei dati può essere designato il Dirigente o un dipendente a tempo indeterminato di questo Ente inquadrato in una categoria non inferiore alla C) ovvero un soggetto esterno, persona fisica o soggetto giuridico. L'assenza di conflitti di interesse anche potenziali con l'esercizio dei propri compiti è strettamente connessa agli obblighi di indipendenza del RPD.

I dati identificativi e di contatto del Responsabile della protezione dei dati sono pubblicati nel sito web istituzionale dell'ente, rendendoli accessibili da un apposito link, comunicati all'Autorità di controllo, comunicati ai componenti degli organi di governo, a tutti i dirigenti e dipendenti comunali, ai componenti degli organi di controllo interni nonché sono inclusi in tutte le informative rese agli interessati ai sensi degli articoli 13 e 14 del GDPR.

PARTE III - ADEMPIMENTI E PROCEDURE

Misure per la sicurezza dei dati personali

Il CdA, i Dirigenti / Responsabili di P.O. e l'Amministratore del sistema informatico provvedono, per quanto di rispettiva competenza, all'adozione ed alla dimostrazione di aver adottato le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza correlato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

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

Registro delle attività di trattamento

Ai sensi dell'articolo 30 del GDPR "*Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità*"; la medesima norma individua il contenuto minimo di tale registro, specificando poi che esso è tenuto in forma scritta, anche in formato elettronico e dev'essere messo a disposizione dell'autorità di controllo.

La tenuta di siffatto registro si configura pertanto come base necessaria al fine di dimostrare la conformità dei trattamenti ai principi enucleati dal GDPR e non soltanto come strumento operativo di mappatura dei trattamenti effettuati.

Un'altra grande differenza rispetto al D.Lgs. 196/2003 è la modalità di mantenimento di tale documento. Non c'è più una scadenza di revisione annuale, ma viene richiesto che il documento sia sempre aggiornato.

L'ente adotta un sistema informatico per meglio consentire l'aggiornamento e l'accesso alle informazioni. Il sistema informatico deve rispettare il contenuto prescritto dal GDPR e deve tener conto delle prescrizioni impartite dal Gruppo ex art. 29 (Ora Comitato europeo per la protezione dei dati) nonché dal Garante per la protezione dei dati personali.

Una elaborazione cartacea del registro è sottoposta all'approvazione della CdA con cadenza almeno annuale mentre una sua copia informatica è posta in conservazione sostitutiva.

In ragione delle dimensioni, anche organizzative di questa Amministrazione, le operazioni tecniche connesse all'istituzione, alla compilazione ed all'aggiornamento delle informazioni contenute nel Registro possono essere demandate ad un fornitore di servizi software esterno, scelto nel rispetto della vigente normativa in materia di appalti pubblici, il quale presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Tale soggetto esterno sarà designato quale Responsabile del trattamento.

Spetta al Titolare, con la collaborazione dei Dirigenti / Responsabili di P.O.:

- effettuare la ricognizione integrale di tutti i trattamenti di dati personali svolti, al fine di consentire la compilazione del registro;

- effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa;
- effettuare l'analisi del rischio dei trattamenti e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli Interessati, da sottoporre all'approvazione del Titolare.

Una importante funzione di controllo in ordine alla regolare tenuta nonché aggiornamento del registro delle attività di trattamento è demandata alla figura del DPO.

Ai sensi dell'art. 39 del GDPR che disciplina infatti le prerogative del Responsabile della protezione dei dati personali si evince che tra le altre è tenuto a "*sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo*". All'attribuzione di controllo che gli viene assegnato direttamente dalla legge si aggiunge il principio di accountability che impone in tal caso al DPO di verificare che l'organizzazione per la quale compie attività di verifica sia conforme alla disciplina del Regolamento non solo in termini di adempimento, ma anche di capacità di dimostrazione della compliance normativa.

Principio di Privacy By Design e By Default (Art. 25 del Regolamento)

Trattasi del principio introdotto dall'art. 25 del Regolamento, ove si prevede che "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Un meccanismo di certificazione approvato ai sensi dell'art. 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo".

Destinatari

I destinatari della procedura sono tutti i dipendenti e collaboratori autorizzati al trattamento dei dati. Ruoli e responsabilità

L'azienda ha adottato il "PIANO DI PROTEZIONE E MODELLO ORGANIZZATIVO A TUTELA DEI DATI PERSONALI", a cui si fa espresso ed integrale rinvio.

Attività operative

Le fasi di attività connesse alla gestione la corretta applicazione dei principi di Privacy by Design e Privacy by Default, si sostanziano in:

1. Mappatura preliminare dei trattamenti eseguiti, delle tipologie di dati trattati e dei soggetti che svolgono operazioni di trattamento
2. Verifica dell'applicabilità dei principi al trattamento
3. Applicazione dei principi al trattamento
4. Modifica o introduzione di un trattamento
5. Archivio della documentazione Mappatura preliminare

Preliminare a qualsiasi ulteriore azione è la mappatura dei trattamenti eseguiti, delle tipologie di dati trattati e dei soggetti coinvolti nelle operazioni di trattamento, effettuata dal Titolare del trattamento.

Tale mappatura permette di ricostruire i flussi di trattamento e così di poter fruire di informazioni utili per la migliore applicazione dei principi in oggetto.

Verifica dell'applicabilità dei principi di Privacy by Design e Privacy by Default

Il Titolare del trattamento verifica la coerenza di ciascun trattamento aziendale ai principi Privacy by Design e Privacy by Default, in relazione ai singoli ambiti di applicazione del GDPR,

Applicazione dei Principi di Privacy by Design e by Default

Ogni qualvolta sia previsto lo sviluppo di un nuovo processo/servizio/strumento o una modifica dello stesso (di finalità), preliminarmente il Titolare del trattamento applica i principi di privacy by design e by default al fine di:

- individuare i dati personali che saranno oggetto di trattamento;
- limitare la raccolta dei dati esclusivamente a quei dati personali realmente necessari per la realizzazione delle finalità perseguite, in ottemperanza al principio di minimizzazione dei dati;
- determinare, sin dall'origine, il periodo di conservazione dei dati; tale periodo è determinato sulla base della durata del trattamento previsto, nonché tenendo conto di eventuali obblighi imposti da norme prevalenti. Qualora fosse impossibile determinare un periodo di conservazione definito, è necessario indicare i criteri adottati per definire i tempi di conservazione;
- individuare i dipendenti e/o collaboratori e/o altri soggetti terzi che, per lo svolgimento delle rispettive attività, avranno accesso ai dati personali, al fine di provvedere alla formalizzazione di appositi documenti di nomina;
- implementare specificisoluzioni, in ottemperanza ai requisiti per la protezione dei dati personali, che possano impedire o limitare eventi di violazione in seguito ad attacchi informatici esterni o comportamenti illeciti interni; tra questi, a titolo esemplificativo, si cita l'estensiva adozione di tecniche di cifratura delle informazioni "a riposo" e in transito, di pseudonimizzazione, di aggregazione dei dati nelle fasi immediatamente successive alla raccolta e sul sistema di origine;

- valutare se il trattamento possa presentare un rischio elevato per i diritti degli interessati.

Per favorire l'applicazione dei principi di privacy by design e by default, allegato al presente documento viene fornita una checklist comprensiva dei controlli di sicurezza.

Contesto	Responsabilità connesse al trattamento		Valutare le responsabilità dei soggetti coinvolti: il titolare del trattamento, gli eventuali responsabili e contitolari
	Standard applicabili al trattamento		Ad es. codici di condotta approvati e certificazioni in materia di protezione dati
	Considerare quali tipi di dati sono oggetto di trattamento		Dati raccolti e trattati in modo sommario
	Ciclo di vita del trattamento		Descrivere il ciclo di vita dei dati (dalla raccolta alla distruzione, passando per la loro conservazione, i vari step del trattamento, l'archiviazione, ecc.)
	Risorse a supporto dei dati oggetto di trattamento		E' necessario considerare le risorse che ospitano i dati oggetto del trattamento (sistemi operativi, server, software, reti, persone, supporti cartacei ecc.)
Principi fondamentali	Gli scopi del trattamento sono specifici, espliciti, legittimi?		
	Basi legali che legittimano il trattamento		Individuare le basi legali del trattamento (ad esempio consenso, esecuzione di un contratto, obbligo legale, interessi vitali ecc.)
	I dati raccolti sono adeguati, pertinenti, limitati a quanto necessario in relazione alle finalità per cui sono trattati?		
	I dati sono esatti e aggiornati?		Considerare le misure previste per garantire la qualità dei dati
	Considerare il periodo di conservazione dei dati		
	Considerare come fornire l'informativa agli interessati		Informazioni che si prevede di fornire agli interessati e strumenti utilizzati a tale scopo
	Se necessario il consenso, considerare tale aspetto e valutare le modalità per ottenerlo		
	Valutare come fanno gli interessati aesercitare i loro diritti (accesso, rettifica, cancellazione, limitazione, portabilità, opposizione)		Fare riferimento alla procedura per l'esercizio dei diritti
	Presenza di Responsabile del Trattamento	Sì No	trattamento di dati personali
Responsabile del trattamento			
	Responsabile del Trattamento UE/Extra UE	Sì No	Indicare se il Responsabile Esterno è collocato in territorio UE o Extra UE
	Trasferimento dati UE/Extra UE	Sì No	Se noto, indicare se il trasferimento di dati personali avviene in territorio UE o Extra UE

	Compliance Privacy del Responsabile del Trattamento		Considerare la sensibilità al tema privacy e il grado di rispetto della normativa del fornitore
	Garanzie di sicurezza offerte dal Responsabile del Tratta-mento		Considerare le misure di sicurezza del for-nitore
Titolari autono-mi	Presenza di comunicazione a Titolari Autonomi	Sì No	Indicare "Sì" se viene effettuato il trasferi-mento di dati personali verso Titolari Auto-nomi
	Titolare UE/Extra UE	Sì No	Indicare se il Titolare Autonomo è colloca-to in territorio UE o Extra UE
	Trasferimento Dati UE/Extra UE	Sì No	Se noto, indicare se il trasferimento di dati personali avviene in territorio UE o Extra UE
Classificazione tipologia di dati	Dati personali	Sì No	Indicare "Sì" se il trattamento prevede l'impiego di dati comuni come per es. nome, cognome, data di nascita, resi-denza, domicilio
	Finanziari / Patrimoniali (cons. 75)	Sì No	Indicare "Sì" se il trattamento prevede l'impiego di dati economico finanziari come i dati relativi al reddito, movimenti di conti corrente, saldi patrimoniali, movimenti titoli ecc.
	Categorie particolari di dati personali (art. 9)	Sì No	Indicare "Sì" se il trattamento prevede l'impiego di dati c.d. sensibili quali 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 o orientamento sessuale
	Dati videosorveglianza	Sì No	
	Dati personali relativi a condanne penali e reati (art. 10)	Sì No	
Sicurezza	Esposizione dati	Sì No	Indicare "Sì" se l'attività di change preve-de l'esposizione su internet/mobile database di dati personali e/o sensibi- li quali nome, cognome, password, fir-me, email, numeri di telefono, etc.
	Piattaforma		Considerare se l'applicazione è di pro-prietà o meno e se sussistono o sono previste attività di customizzazione
	Tipologia utenti		Considerare la tipologia di utenti utilizza-tori dell'applicazione
	Ambiente di deploy		Considerare gli ambienti in cui è installa-ta l'applicazione: Sviluppo, Test, Pro-duzione

	Linguaggio di programmazione Anonimizzazione/Pseudonimizzazione dati		Considerare se il linguaggio di programmazione in cui è sviluppata l'applicazione
	Detenzione del codice sorgente	Sì No	Indicare "Sì" se si possiedono fisicamente i codici sorgente dell'applicazione

	Installazione		Considerare se si tratta di un'applicazio- ne client o server
	Sistema di autenticazione		Considerare il sistema di autenticazione utilizzato dall'applicazione
	Certificazioni		Considerare la certificazione cui è soggetta l'applicazione
	Cifratura database		Indicare "Sì" se il database utilizzato è protetto da procedure di cifratura
	Anonimizzazione/Pseudonimizzazione dati		Indicare "Sì" se i dati sono protetti da procedure di anonimizzazione/pseudonimizzazione

Valutazioni di impatto sulla protezione dei dati

Nel caso in cui una tipologia di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, con la collaborazione del Dirigente / Responsabile di P.O. competente in relazione al trattamento interessato, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

La valutazione dell'impatto del medesimo trattamento (DPIA) è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi. Un processo di DPIA può riguardare una singola operazione di trattamento dei dati. Tuttavia, si potrebbe ricorrere a un singolo DPIA anche nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Ciò potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Oppure, un singolo processo di DPIA potrebbe essere applicabile anche a trattamenti simili attuati da diversi titolari del trattamento dei dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile un DPIA di riferimento, attuare le misure descritte nello stesso, e fornire una giustificazione per la realizzazione di un unico DPIA.

Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dall'Autorità di controllo ai sensi dell'art. 35, paragrafi 4-6, del GDPR.

La DPIA deve essere effettuata prima di procedere al trattamento, già dalla fase di progettazione del trattamento stesso anche se alcune delle operazioni di trattamento non sono ancora note, in coerenza con i principi di privacy by design e by default per determinare se il trattamento deve prevedere misure opportune in grado di mitigare i rischi.

L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione

di soluzioni che promuovono la conformità. Il Titolare conduce quindi una prima fase di valutazione preliminare, il cui scopo è quello di raccogliere tutte le informazioni necessarie a valutare prima di tutto se il trattamento sia conforme al GDPR e, in seconda battuta, comprendere se quel trattamento debba essere sottoposto ad una valutazione DPIA. L'attività quindi si scompone di 3 sotto fasi:

a. descrizione del trattamento (le categorie di soggetti interessati dal trattamento, le finalità del trattamento, le categorie di dati oggetto del trattamento, le modalità di trattamento, il luogo di conservazione dei dati trattati, …) sulla scorta delle risultanze contenute nell'apposito registro;
b. valutazione della conformità (analisi della necessità e della proporzionalità del trattamento rispetto alle finalità; rispetto dei principi applicabili al trattamento di cui al capo II del GDPR; rispetto dei diritti degli interessati di cui al capo III del GDPR);
c. valutazione della obbligatorietà di condurre una DPIA.

Fermo restando quanto indicato dall'art. 35, paragrafo 3, del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del GDPR;
e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare, sentito il Responsabile della protezione dei dati e l'Amministratore del sistema informatico (se esistente), ritenga motivatamente che non possa presentare un rischio elevato.

Il Titolare, motivatamente, ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

La DPIA non è necessaria nei casi seguenti:

a) se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, paragrafo 1, del GDPR;

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 25 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.

Non è inoltre necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte dell'Autorità di controllo o dal Responsabile della protezione dei dati personali e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni dell'Autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate. Una volta determinata la necessità di procedere ad una attività di DPIA si rende necessario procedere alla raccolta delle informazioni necessarie allo sviluppo successivo delle attività di analisi dei rischi e produzione del piano dei trattamenti.

L'attività si scompone in ulteriori 4 sotto fasi:

a. raccolta delle informazioni per l'analisi dei rischi (informazioni presenti all'interno dei trattamenti, procedimenti coinvolti dal trattamento, finalità dei dati raccolti, flussi informativi, autorizzati all'accesso alle informazioni, asset model a sostegno dei trattamenti (applicativi, hardware, reti, ecc.). Le valutazioni che dovranno essere fatte durante la fase di analisi dei rischi devono tenere in considerazione;
a) due aspetti fondamentali: sia i rischi derivanti dai contenuti intrinseci del trattamento stesso comprendenti soprattutto modalità e finalità sia i rischi derivanti da possibili violazioni di sicurezza della protezione del dato);
b. valutazione dei rischi, di norma sviluppata nel classico concetto di valutazione degli impatti e probabilità afferenti ad una serie di minacce in grado di compromettere un asset (informativo) (alcuni esempi sono gli impatti derivanti da una violazione della sicurezza fisica; da una violazione dei dati di identificazione o attinenti l'identità personale; perdite finanziarie o al patrimonio, perdite dovute a frodi; turbamento per la diffusione di una notizia riservata, compromissione di uno stato di salute, evento lesivo dei diritti umani inviolabili o dell'integrità della persona; conseguenze di tipo discriminatorio, perdite di autonomia);
c. valorizzazione delle contromisure e rischio residuo. L'associazione di minacce e contromisure esistenti consente a questo punto di determinare il rischio effettivo che sarà confrontato con un valore di rischio accettabile;
d. piano di trattamento dei rischi.

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

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:
    1) delle finalità specifiche, esplicite e legittime;
    2) della liceità del trattamento;
    3) dei dati adeguati, pertinenti e limitati a quanto necessario;
    4) del periodo limitato di conservazione;
    5) delle informazioni fornite agli interessati;
    6) del diritto di accesso e portabilità dei dati;
    7) del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;

8) dei rapporti con i responsabili del trattamento;
9) delle garanzie per i trasferimenti internazionali di dati;
10) consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;
e) l'acquisizione del parere del Responsabile della protezione dei dati personali.

Assume quindi fondamentale importanza l'attività di formalizzazione dei risultati la quale consiste nel valutare se le misure individuate sono idonee a mitigare i rischi ad un livello accettabile, stimando in tal senso un rischio residuo, nonché documentare i risultati di tutte le attività svolte durante la DPIA ed i razionali che determinano la scelta se procedere o meno alla Consultazione Preventiva.

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, devono concorrere alla realizzazione di un documento finale in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dal GDPR. Il documento deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

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

Il Titolare, in relazione al trattamento interessato, garantisce l'effettuazione della DPIA ed è responsabile della stessa, salvo che ne affidi l'esecuzione ad altro soggetto, anche esterno all'Ente.

Il Titolare in relazione al trattamento interessato deve consultarsi con il Responsabile della protezione dei dati personali anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare in relazione al trattamento interessato devono essere documentate nell'ambito della DPIA.

Il Titolare deve consultare l'Autorità di controllo prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato (tale obbligo è previsto se si ritiene che il trattamento sottoposto a DPIA violi il GDPR, in particolare qualora non si abbia identificato o attenuato sufficientemente il rischio). Il Titolare consulta l'Autorità di controllo anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

Quando è stata richiesta una valutazione preventiva all'Autorità di Controllo il trattamento non può essere iniziato almeno fino a che in procedimento di consultazione preventiva si è concluso con successo.

Salvo diversa disposizione dell'Autorità di controllo è bene che la comunicazione di richiesta di consultazione avvenga con modalità che consentano di dimostrare la data certa della stessa comunicazione (es. PEC, Raccomandata, ecc.) visto che i tempi stabiliti per lo sviluppo del processo di consultazione preventiva decorreranno da tal data. L'attività include il recepimento dell'eventuale risposta e l'attuazione degli eventuali interventi necessari per aderire al parere fornito dall'Autorità.

Il processo DPIA deve sempre prevedere un monitoraggio dei risultati raggiunti ed un conseguente e costante riesame al fine di garantire nel tempo la mitigazione dei rischi e la conformità al GDPR, anche a fronte di

fisiologici cambiamenti a cui sono soggetti tutti i trattamenti (contesto interno ed esterno, finalità del trattamento, strumenti utilizzati, organizzazione, presenza di nuove minacce, ecc.).

Il Responsabile della protezione dei dati personali monitora lo svolgimento della DPIA. Può inoltre proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Eventuali Responsabili del trattamento collaborano e assistono il Titolare oltre che il Responsabile della protezione dei dati nella conduzione della DPIA fornendo ogni informazione necessaria. L'Amministratore del sistema informatico (se designato) fornisce il necessario supporto al Titolare per lo svolgimento della DPIA. Può inoltre proporre di condurre una DPIA in relazione ad uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

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

Dal punto di vista operativo - considerata la complessità di un processo DPIA e relativa fase di analisi dei rischi – il Titolare deve adottare strumenti applicativi specializzati in grado di gestire tutte le fasi del processo ed in grado di riproporre la sua applicabilità nel tempo.

Un esempio di un software applicativo per la gestione di un processo DPIA è "PIA", scaricabile gratuitamente dal sito di CNIL (Autorità francese per la protezione dei dati). Il software, al quale ha aderito anche il garante Italiano, non costituisce un modello al quale fare sempre riferimento (si ricorda che è stato concepito soprattutto per le PMI), ma può offrire un focus sugli elementi principali di cui si compone la procedura di DPIA. Può quindi costituire un utile supporto metodologico e di orientamento allo svolgimento di una DPIA, ma non va inteso come schema predefinito per ogni valutazione d'impatto che va integrata in ragione delle tipologie di trattamento esaminate. Può servire inoltre per comprendere meglio quali possono essere i requisiti di base di un applicativo DPIA adeguato alla propria realtà procedendo quindi ad una software selection più mirata e consapevole.

Violazione dei dati personali

Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporti, accidentalmente od 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 (tale indicazione operativa pertanto si applica a tutti gli archivi/documenti cartacei ed a tutti i sistemi, anche informativi sui quali siano conservati i dati personali degli interessati, quali cittadini, dipendenti, fornitori, soggetti terzi, ecc.).

La segnalazione di un possibile Data Breach può provenire dall'esterno (cittadini, fornitori esterni, enti istituzionali ecc.) o dall'interno, da parte delle varie funzioni di settore durante il normale svolgimento dell'attività lavorativa (più frequentemente tali eventi vengono evidenziati da funzioni che svolgono attività di verifica e /o di controllo).

Colui il quale riceve la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di violazione di dati personali, deve darne immediata notizia al Titolare il quale, con la collaborazione del Dirigente / Responsabile di P.O. competente, deve:

- adottare le misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informa immediatamente il Responsabile della Protezione dei Dati per una valutazione condivisa;

- condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) attraverso la compilazione del "Modello di potenziale violazione di dati personali al Responsabile Protezione Dati" **(Allegato 1)**;
- riferire i risultati dell'indagine inviando il modello al Responsabile della Protezione dei Dati.

Il Responsabile della Protezione dei Dati, ricevuti i risultati dell'indagine, analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante. Lo invia quindi al Titolare.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione all'Autorità di controllo. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Qualora la notifica effettuata nelle 72 ore non sia completa è possibile integrarla in una o più fasi successive (ad es. nel caso di violazioni complesse per le quali occorrono indagini approfondite) corredandola con i motivi (analogamente come in caso di notifica in ritardo). Nel caso in cui la scoperta della violazione non sia contestuale al verificarsi dell'evento che l'ha generata, devono essere indicate nella comunicazione le motivazioni che non hanno consentito l'immediata rilevazione dell'evento stesso e le misure adottate o che si intende adottare affinché ciò non si ripeta in futuro.

Il Responsabile del trattamento eventualmente coinvolto deve:

a) informare il Titolare tempestivamente ed in ogni caso entro e non oltre 24 ore dalla scoperta dell'evento, tramite PEC, di essere venuto a conoscenza di una violazione e fornire tutti i dettagli della violazione subita, in particolare una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sull'Ente e sugli Interessati coinvolti e le misure adottate per mitigare i rischi;
b) fornire assistenza per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli Interessati coinvolti. Il Titolare si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito. Risulta opportuno e di particolare importanza che tutti gli atti di designazione a Responsabile del trattamento contengano una espressa previsione circa la necessità di informare l'ente, senza ingiustificato ritardo, in caso di avvenuta conoscenza di una violazione di dati personali, anche solo probabile o possibile.

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

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

Ove il Titolare ritenga che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata sia elevato, deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. Prima di procedere alla comunicazione della violazione ai soggetti interessati il testo della comunicazione, le modalità di notifica e le evidenze che attestano il reale livello di pregiudizio, dovranno essere concordate con il Responsabile della protezione dei dati personali. Nel caso in cui la comunicazione dovesse pregiudicare lo svolgimento delle verifiche

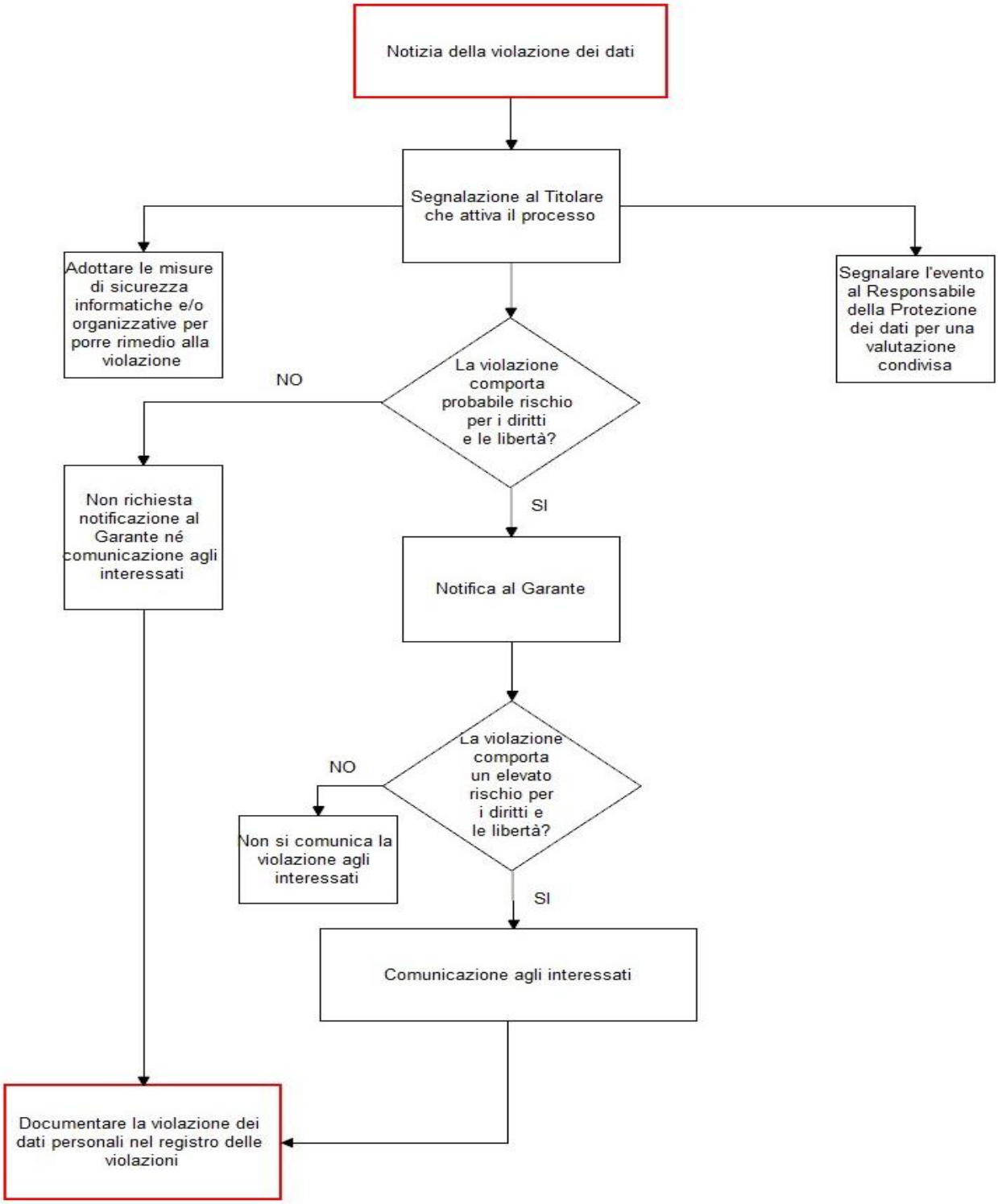
sull'evento Data Breach, il Titolare può chiedere all'Autorità di controllo l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento di tali verifiche.

La probabilità e la gravità del rischio, per i diritti e le libertà dell'interessato, dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

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

La notifica all'Autorità di controllo deve avere il contenuto minimo previsto dall'art. 33 del GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al su citato art. 33. Ciascun ufficio 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. E' comunque opportuno che l'inventario delle violazioni tenga traccia anche delle varie fasi di gestione dell'evento, dalla rilevazione, all'analisi e alla sua risoluzione e conclusione. L'inventario dovrà essere dotato di idonee misure di sicurezza atte a garantire l'integrità e l'immodificabilità dei dati in esso registrati. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dall'Autorità di controllo al fine di verificare il rispetto delle disposizioni del GDPR.

Flusso degli adempimenti in caso di violazione dei dati



PARTE IV - DIRITTI DELL'INTERESSATO

Informativa, comunicazione e modalità trasparenti per l'esercizio dei diritti dell'interessato

L'ente adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR nonché per gestire le comunicazioni in merito all'esercizio dei diritti riconosciuti dal GDPR in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni di cui agli articoli 13 e 14 del GDPR sono fornite mediante predisposizione di idonea pagina web sul sito istituzionale.

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'Ente è predisposta apposita informativa. Una informativa breve è fornita, mediante idonei strumenti:
attraverso appositi moduli da consegnare agli interessati. Nel modulo sono indicati i soggetti ai quali l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti, anche al fine di consultare l'elenco aggiornato dei responsabili;

- in avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture comunali, nelle sale d'attesa ed in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet del titolare;
- in apposita avvertenza inserita nei contratti ovvero nelle lettere di affidamento di incarichi del personale dipendente, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, dei tirocinanti, dei volontari, degli stagisti ed altri soggetti che entrano in rapporto con l'ente;
- in apposita avvertenza inserita nelle segnalazioni di disservizio e, in genere, in tutte le comunicazioni dirette all'Amministrazione;
- resa in sede di pubblicazione dei bandi, avvisi, lettere d'invito, ecc..

Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

L'ente agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 12 a 18 del GDPR. Nei casi di cui all'articolo 11, paragrafo 2, del GDPR l'ente non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 12 a 18, salvo che dimostri che di non essere in grado di identificare l'interessato.

L'ente fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta di esercizio dei diritti riconosciuti dal GDPR, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. L'ente informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato. Se non ottempera alla richiesta dell'interessato, l'ente informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese sulla base dei diritti riconosciuti dal GDPR sono gratuite.

Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, l'ente può:

a. addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b. rifiutare di soddisfare la richiesta.
Incombe all'ente l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
Fatto salvo l'articolo 11 del GDPR, qualora l'ente nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di esercizio dei diritti riconosciuti dal GDPR, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

Regole comportamentali relative al trattamento dei dati personali

Art. 1. Principi generali

1. Le presenti norme sono volte a contemperare i diritti fondamentali della persona con l'esercizio delle attività di cura sanitaria e interventi socio sanitari

2. In forza dell´art. 32 della Costituzione, l'esercizio della tutela della salute intesa come situazione di benessere psico fisico e sociale della persona è un bene fondamentale tutelato. L'esercizio delle attività di cura e attività correlate deve essere posto sotto la direzione e diretta responsabilità di un professionista tenuto al segreto professionale.

Su questi principi trovano fondamento il dettato del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (di seguito "Regolamento") e dal d.lgs. 30 giugno, 2003, n. 196 (Codice in materia di protezione dei dati personali, di seguito "Codice"), così come modificato dal d.lgs. 10 agosto 2018, n. 101.

3. I lavoratori sono tenuti a mantenere il segreto sulle informazioni di cui sono venuti a conoscenza durante lo svolgimento delle proprie mansioni.

Art. 2. Banche dati in uso e tutela degli archivi

1. L'ente titolare del trattamento è tenuto a fornire l'informativa di cui agli artt. 13 e 14 del Regolamento, e ha regolare i rapporti con i responsabili e autorizzati al trattamento nonché ad assumere tutte le necessarie misure di protezione ai sensi dell'art.32 del regolamento.

2. I dati personali possono essere raccolti presso l'interessato ovvero presso i propri congiunti, sono raccolti dati anche presso altri enti assistenziali, territoriali e dalla Ulss di competenza. L'ente è tenuto a pubblicare (rendere noti) i contatti dove è possibile esercitare i diritti previsti dal Regolamento.

3. Gli archivi dell'ente, comunque funzionali all'esercizio dell'attività di assistenza socio sanitaria e attività amministrative ed alberghiere collegate, e per l'esclusivo perseguimento delle relative finalità, sono tutelati, ai sensi del Regolamento, nonché del Codice "privacy" e dalle norme del codice civile.

4. L'ente deve conservare i dati per un periodo non definito come previsto dalle normative sui dati sanitari, e sui dati e archivi detenuti dalle pubbliche amministrazioni, approntando tutte le misure appropriate atte ad evitare danni alla riservatezza, disponibilità ed integrità dei dati. È compito dell'amministrazione garantire, con misure tecniche ed organizzative adeguate, l'esattezza del dato. la minimizzazione ove necessario, e altre tecniche di conservazione rispettose delle previsioni delle regole operanti in ambito europeo, e italiano, nonché delle prassi in materia. È compito dell'amministrazione garantire la resilienza delle dotazioni, fisiche ed informatiche, utilizzate per il trattamento, adeguandole alle soluzioni tecniche adeguate.

Art. 3. Tutela dell'Ospite

1.La tutela dell'Ospite residente nell'ente, è l'obiettivo primario dell'amministrazione e del personale ivi impiegato, a qualsiasi titolo. I luoghi di cura, o riabilitazione, devono essere protetti da danni, voluti o accidentali, nel rispetto della possibilità di partecipazione dell'anziano ai trattamenti che lo coinvolgono, al rispetto dei diritti e delle libertà personali, con tutela del corpo fisico e del corpo "elettronico"[1], nel rispetto della dignità della persona.

2. Al fine di tutelarne la personalità, il personale dipendente non fornisce a terzi, particolari in grado di condurre alla identificazione delle persone.

3. La tutela della personalità dell'anziano si estende a tutti i fatti.

4. Il diritto dell'anziano alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di informazione; qualora, tuttavia, per motivi di rilevante interesse pubblico e fermo restando i limiti di legge, l'ente decida di diffondere notizie o immagini riguardanti gli ospiti, dovrà farsi carico della responsabilità di valutare se la pubblicazione sia davvero nell´interesse oggettivo dell'anziano, secondo i principi e i limiti stabiliti dalla legge e della protezione dei dati personali con particolare attenzione alla tutela dei diritti e delle libertà personali.

Art. 4. Rettifica

1. L'ente, attraverso il personale autorizzato, corregge senza ritardo errori e inesattezze, anche in conformità al dovere di rettifica nei casi e nei modi stabiliti dalla legge, e ne dà, tempestivamente, comunicazione agli enti e servizi collegati alle attività di cura, e attività amministrative, nonché agli interessati o loro rappresentanti.

Art. 5. Diritto all'informazione e dati personali

1. Nel raccogliere dati personali atti a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesioni a partiti, sindacati, associazioni o organizzazioni a carattere

[1] Corpo formato dai dati personali

religioso, filosofico, politico o sindacale, nonché dati genetici, biometrici intesi a identificare in modo univoco una persona fisica e dati atti a rivelare le condizioni di salute e la sfera sessuale, l'ente garantisce rispetto dell´essenzialità dell´informazione, evitando riferimenti a congiunti o ad altri soggetti non interessati.

2. Tutte le informazioni raccolte, presso l'interessato o presso terzi, sono meritevoli di massima tutela.

Art. 6. Essenzialità dell'informazione

1. La divulgazione di notizie è vietata.

2. La sfera privata delle persone deve essere rispettata se le notizie o i dati non hanno alcun rilievo sull'attività di assistenza socio-sanitaria ed amministrativa.

3. Commenti e opinioni appartengono alla libertà di informazione nonché alla libertà di parola e di pensiero costituzionalmente garantita a tutti, il dipendente è tenuto, altresì, a mantenere il segreto professionale, su tutte le informazioni di cui venga a conoscenza nell'esercizio delle proprie funzioni, nei limiti del presente atto e delle prescrizioni del Titolare del trattamento.

Art. 7. Tutela della dignità delle persone

1. Salva l'essenzialità dell'informazione, l'ente e i lavoratori non forniscono notizie o pubblicano dati degli ospiti, lesivi della dignità della persona.

2. I dati, in nessun caso, possono essere utilizzati a scopo di lucro.

Art. 8. Tutela del diritto alla non discriminazione

1. Nel condividere informazioni per la realizzazione delle cure e delle attività collegate, il dipendente è tenuto a rispettare il diritto della persona alla non discriminazione per razza, religione, opinioni politiche, sesso, condizioni personali, fisiche o mentali.

Art. 9. Tutela della dignità delle persone malate

1. Il dipendente, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignità, il diritto alla riservatezza e al decoro personale, specie nei casi di malattie gravi o terminali, e si astiene dal diffondere dati di interesse strettamente clinico.

Art. 10. Tutela della sfera sessuale della persona

1. Il dipendente si astiene dalla descrizione di abitudini sessuali riferite ad una determinata persona, identificata o identificabile.

Art. 11. Utilizzo di dotazioni personali

1. E’ vietato utilizzare dotazioni personali (digitali, analogiche, cartacee o altri supporti durevoli) per rilevare dati personali degli anziani residenti nella struttura.

2. L’utilizzo di mezzi di sorveglianza o rilevazione, all’interno dei locali e delle aree di pertinenza, è possibile previa autorizzazione del vertice dell’ente, e accordo sottoscritto con le OO.SS. o con l’Ispettorato Nazionale del Lavoro.

3. E’ vietato realizzare video, fotografie e rilevare l’audio con dispositivi personali. Il Titolare può autorizzare, con atto scritto, in particolari casi tali rilevazioni e o registrazioni.

4. E’ vietato utilizzare i dati degli ospiti (comuni e categorie particolari), per comunicazione o diffusione, a mezzo web o social network.

Art. 12. Ambito di applicazione, sanzioni disciplinari

1. Le presenti norme si applicano a tutti i lavoratori, volontari, persone che a qualsiasi titolo, con o senza remunerazione, operano all’interno dei locali e pertinenze dell’ente.

2. In caso di violazioni, le sanzioni disciplinari e la procedura di cui alla L.300/1970 art. 7, si applicano a tutti soggetti di cui al comma 1 del presente articolo.

3. Spetta al Titolare del trattamento (o suo delegato) irrogare le sanzioni.

Allegato - Potenziale violazione di dati personali - Modello di comunicazione al responsabile della protezione dei dati (Near Miss)

CASA DI RIPOSO
CARTIGLIANO

Titolare

_____	_____	_____
nome e cognome	*tel.*	*e-mail*

Breve descrizione della violazione dei dati personali

Denominazione della/e banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

☐ Il _____
☐ Tra il _____ e il _____
☐ In un tempo non ancora determinato
☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio: tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)
☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
☐ Furto (i dati non sono più sui sistemi del titolare ma sono in possesso dell'autore della violazione)
☐ Altro _____

Dispositivo o strumento oggetto della violazione

☐ Computer
☐ Rete
☐ Dispositivo mobile
☐ File o parte di un file
☐ Strumento di backup
☐ Documento cartaceo
☐ Software _____
☐ Servizio informatico _____
☐ Altro _____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

☐ Numero _____ di persone
☐ Circa _____ persone
☐ Un numero (ancora) sconosciuto di persone