COMUNE DI ORISTANO

PIANO DI PROTEZIONE DEI DATI PERSONALI E GESTIONE DEL RISCHIO DI VIOLAZIONE 2020/2022

Approvato con Deliberazione n° 290 del 24/12/2019

SOMMARIO

RIFERIMENTI DOCUMENTALI

Titolo del Documento	Piano di protezione dei dati personali
Numero di versione	001
Data ultimo aggiornamento	20.12.2019
Stato del documento	
Estensori del documento	Servizio Privacy e CED
Riferimento per comunicazioni in merito al documento	trasparenza@comune.oristano.it
Modalita' di distribuzione del presente documento e delle eventuali nuove versioni	invio RPD e pubblicazione successiva sul sito

PREMESSA

La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L"articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell"Unione europea ('Carta') e l'articolo 16, paragrafo 1, del Trattato sul funzionamento dell"Unione europea ('TFUE') stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche. Senonché', la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali.

La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l"economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell"Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

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 ñal fine di soddisfare i requisitiò 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 lôimportanza della normativa e di ciò che essa mira a proteggere, la migliore risposta in termini di cambiamento organizzativo sia quella di realizzare un complessivo ñModello organizzativo e di gestioneò per la protezione dei dati personali, considerando come tale un complesso di attività organizzativa, di ruoli, di azioni organizzative, di sistemi mirato al fine dellôapplicazione ñordinataò e completa, nellôazione amministrativa dellôEnte, 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. Lôadeguamento al Regolamento UE 2016/679 impone al Titolare di trattamento pubblico di prestare grande attenzione al fattore organizzativo. Per questo, lôapprovando 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 allôorganizzazione del personale operante allôinterno dellôEnte, nelle sue articolazioni gerarchiche. Eô ammesso ed anzi incoraggiato lôutilizzo 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

PIANO DI PROTEZIONE DEI DATI PERSONALI (PPD)

DEFINIZIONI

Il presente documento recepisce e utilizza le seguenti definizioni:

GDPR: il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR generale sulla protezione dei dati);

PPD: il presente Piano di Protezione dei Dati personali e gestione del rischio di violazione;

DATA BREACH: ñriuscire a fare brecciaò, 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 ñrendere contoò, 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 dellôamministrazione ha verso chi lôha scelta e si fonda su: trasparenza intesa come informazioni dellôattività di governo; partecipazione di chiunque al miglioramento delle politiche pubbliche e collaborazione intesa come efficacia dellôazione amministrativa attraverso la cooperazione tra tutti i livelli di governo

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato'); si considera identificabile la persona fisica che puo' essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o piu' elementi caratteristici della sua identita' fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

TRATTAMENTO: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

LIMITAZIONE DEL TRATTAMENTO: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

PROFILAZIONE: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per

analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, lôaffidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

PSEUDONIMIZZAZIONE: il trattamento dei dati personali in modo tale che i dati personali non possano piu' essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

ARCHIVIO: qualsiasi insieme di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

TITOLARE DEL TRATTAMENTO: la persona fisica o giuridica, l'autorita' pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalita' e i mezzi del trattamento di dati personali. Ai fini del presente Piano il titolare del trattamento è il Comune di Oristano nella persona del Sindaco Pro Tempore quale rappresentante dellôEnte;

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

DESTINATARIO: la persona fisica o giuridica, l'autorita' pubblica, il servizio o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorita' pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorita' pubbliche e' conforme alle norme applicabili in materia di protezione dei dati secondo le finalita' del trattamento;

TERZO: la persona fisica o giuridica, l'autorita' pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile;

VIOLAZIONE DEI DATI PERSONALI: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

DATI GENETICI: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

DATI BIOMETRICI: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

DATI RELATIVI ALLA SALUTE: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

RAPPRESENTANTE: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o da responsabile del trattamento per iscritto ai sensi dell'articolo 27 del GDPR, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

AUTORITA' DI CONTROLLO: lôautorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR;

OGGETTO

Il PPD 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 ridurre/eliminare il rischio di violazione dei dati derivante dal trattamento.
In tale quadro, il documento disciplina, il processo di gestione del rischio di violazione dei dati personali:

- comuni;
- sensibili;
- giudiziari.

La disciplina si applica ai:

1.trattamenti con strumenti elettronici;
2.trattamenti senza l'ausilio di strumenti elettronici (ad esempio: cartacei, audio, visivi e audiovisivi, ecc.).

Per quanto concerne i trattamenti con strumenti elettronici, secondo il D.Lgs. n. 196/2003, tale trattamento e' consentito solo se sono adottate, le seguenti misure minime:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;

Per quanto concerne i trattamenti senza l'ausilio di strumenti elettronici, secondo il D.Lgs. n. 196/2003, tale trattamento è consentito solo se sono adottate, le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

FINALITA'

Il presente documento, in attuazione del GDPR e della normativa interna di adeguamento, è funzionale alla protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali trattati nell'esercizio dellôattività istituzionale in un quadro di garanzie per gli interessati che contempla nuovi diritti. Sul presupposto che costituisce un obiettivo strategico la sicurezza del trattamento dei dati personali, scopo del presente documento è programmare e pianificare gli interventi affinché' i dati personali siano:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ('liceità', correttezza e trasparenza');

b) 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'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali ('limitazione della finalità');

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ('minimizzazione dei dati');

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ('esattezza');

e) 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 piu' 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'articolo 89, paragrafo 1, fatta salva l'adeguamento di misure tecniche e organizzative adeguate richieste dal presente GDPR a tutela dei diritti e delle liberta' dell'interessato ('limitazione della conservazione');

f) 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 ('integrità' e riservatezza').

QUADRO NORMATIVO DI RIFERIMENTO

Il PPD tiene conto dei seguenti documenti:

- Codice in materia di dati personali (D.Lgs. n.196/2003);
- Linee guida e raccomandazioni del Garante;
- GDPR UE 679/2016 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- Legge 25 ottobre 2017, n. 163 (art.13), recante la delega per l'adeguamento della normativa nazionale alle disposizioni del GDPR (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- D.Lgs. n. 101/2018 di adeguamento della normativa interna al GDPR;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN
- Linee guida adottate dal Gruppo di lavoro Art. 29;
- Norme internazionali;
- Regolamenti interni, approvati dai titolari e/o dai responsabili.

CORRELAZIONE CON GLI ALTRI STRUMENTI DI PIANIFICAZIONE

La violazione dei dati personali, intesa come violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, è rilevante ai fini del piano triennale per la prevenzione della corruzione e per la trasparenza e degli altri strumenti di programmazione dell'ente, in particolare il documento unico di programmazione e il piano delle performance.

La correlazione tra i diversi strumenti di programmazione sopra richiamati viene garantita in fase di elaborazione, attraverso lôinserimento di appositi obiettivi strategici, operativi e gestionali, e, in fase di adeguamento, attraverso il costante monitoraggio sullo stato di attuazione degli stessi.

DATA E PROVVEDIMENTO DI APPROVAZIONE

La Giunta Comunale, organo competente del titolare del trattamento, ha approvato il PPD con delibera nr. **290** del **24 dicembre 2019**.

PERIODO DI RIFERIMENTO E MODALITA' DI AGGIORNAMENTO

Il PPD copre il periodo del triennio 2020-2022, e la funzione principale dello stesso e' quella di assicurare il processo, a ciclo continuo, di adozione, modificazione, aggiornamento e adeguamento del processo di gestione del rischio e della strategia di sicurezza, secondo i principi, le disposizioni e le linee guida elaborate a livello nazionale e internazionale.
Il documento consente che la strategia si sviluppi e si modifichi in modo da mettere via via a punto degli strumenti di protezione mirati e sempre più incisivi.

In questa logica, l'adozione del documento non si configura come unâattività una tantum, bensì come un processo continuo in cui le strategie e gli strumenti vengono via via affinati, modificati o sostituiti in relazione al feedback ottenuto dalla loro applicazione.

Eventuali aggiornamenti successivi, anche infra annuali, correlati agli esiti dei monitoraggi o alla sopravvenienza di nuove normative o prassi, sono oggetto di approvazione da parte dello stesso organo che ha approvato il PPD.

PARTE II

DATI PERSONALI, RISCHIO DI VIOLAZIONE E DISCIPLINA

Nell'attuale contesto, lo sviluppo e la rapidità dell'evoluzione tecnologica nonché' la globalizzazione comportano nuove sfide per la protezione dei dati personali. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. Nel contempo, la tecnologia attuale consente a soggetti pubblici e privati di utilizzare dati personali come mai in precedenza, e la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati, tenuto conto dell'aumento del rischio di violazione dei dati medesimi e della necessità che le persone fisiche abbiano il controllo dei dati personali che li riguardano in un quadro di certezza giuridica e operativa rafforzata così come delineata del GDPR.

Il rischio inerente al trattamento è da intendersi come rischio di impatti negativi sulle libertà e sui diritti degli interessati.

Rispetto a tali possibili impatti negativi, il Comune di Oristano promuove e adotta approcci e politiche che tengono conto costantemente del rischio, effettuando una analisi attraverso un apposito processo di valutazione che tiene conto:

- dei rischi noti o evidenziabili;
- delle misure tecniche e organizzative adottate o che si intende adottare per mitigare il rischio.
- l'obbligo di effettuare valutazioni di impatto (DPIA) prima di procedere ad un trattamento di dati che presenti rischi elevati per i diritti delle persone, e di consultare lôAutorità di protezione dei dati in caso di dubbi;
- adeguate misure di sicurezza;
- un sistema di monitoraggio sull'efficacia delle misure;
- la figura del "Responsabile della protezione dei dati" (RPD/DPO).

LA CONFIGURAZIONE DEL SISTEMA DI PROTEZIONE COME PROTEZIONE FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

Tenendo conto dello stato dell'arte e dei costi di adeguamento, nonché' della natura, dell'ambito di applicazione, del contesto e 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, l'Ente in persona del titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte a:

- attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione;
- integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR, e tutelare i diritti degli interessati;
- garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, garantendo che non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Il principio chiave è sintetizzato dall'espressione inglese "data protection by default and by design" (si veda art. 25 GDPR), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del GDPR 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.

Tutto questo va effettuato a monte, prima di procedere al trattamento dei dati vero e proprio e richiede, pertanto, un'analisi preventiva e un impegno applicativo che devono sostanziarsi in una serie di attività specifiche documentabili e dimostrabili.

Il delineato sistema di protezione vale per:

- la quantità dei dati personali raccolti;
- la portata del trattamento;
- il periodo di conservazione;
- lôaccessibilità.

L'ACCOUNTABILITY QUALE CONSEGUENZA DELL'APPROCCIO BASATO SUL RISCHIO

Il sistema di protezione "by default and by design" si fonda sull'assunto che il titolare del trattamento o un suo delegato:

- è competente per il pieno e rigoroso rispetto del sistema di protezione dei dati personali e, in particolare, per il rispetto dei principi di "liceità', correttezza e trasparenza", "limitazione della finalità", "minimizzazione dei dati", "esattezza", "limitazione della conservazione" e "integrità e riservatezza";

- e' in grado di comprovare il rispetto del sistema di protezione e dei relativi principi in base al principio di "responsabilizzazione" (accountability).

In tale modo viene affidato al titolare 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 specifici indicati nel GDPR.

Sulla base di tale impostazione, il GDPR pone con forza l'accento sulla "responsabilizzazione" (accountability) del titolare e dei responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR.

Accountability: Registro e ricognizione dei trattamenti

Il Comune di Oristano ha istituito e tiene costantemente aggiornato, in forma scritta, anche elettronica il registro delle operazioni di trattamento che costituisce lo strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Ente, indispensabile per ogni valutazione e analisi del rischio. La tenuta del registro dei trattamenti non costituisce un adempimento formale bensi' parte integrante di un sistema di corretta gestione dei dati personali.

A fini della istituzione e della tenuta del registro, il titolare del trattamento compie e tiene costantemente aggiornata un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

Accountability: Misure di sicurezza

In relazione al principio di responsabilizzazione lôEnte valuta l'adeguato livello di sicurezza da adottare, tenendo conto dei rischi che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

La valutazione in ordine alla concreta identificazione e adeguamento delle misure e' rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del GDPR. **Per tale motivo, dopo il 25 maggio 2018, sono venuti meno obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 D.Lgs. n. 196/2003).**

Accountability: Notifica delle violazioni di dati personali

in caso di violazione dei dati personali lôente notifica la violazione allôautorità di controllo competente a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le liberta' delle persone fisiche. Se la probabilita' di tale rischio e' elevata, e' necessario informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo" ferme restando le eccezioni costituite dalle circostanze indicate al paragrafo 3 dell'art. 34 del GDPR.

I contenuti della notifica allôautorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli artt. 33 e 34 del GDPR e dalla normativa interna di adeguamento.

Accountability: Responsabile della protezione dei dati

L'approccio di responsabilizzazione proprio del GDPR, si riflette anche nellôobbligo di designare un "responsabile della protezione dati" (RPD/DPO), quale figura indipendente, autorevole, dotata di competenze manageriali e tenuta al segreto d'ufficio, finalizzata a facilitare l'adeguamento del GDPR da parte del titolare e del responsabile. Pertanto lôEnte ha provveduto a nominare il proprio RPD con decreto del Sindaco n. 28 del 22 maggio 2018.
I dati identificativi e di contatto del Responsabile della protezione dei dati sono pubblicati nel sito web istituzionale dellôEnte, resi accessibili da un apposito link e comunicati allôAutorità di controllo.

Il SISTEMA DI PROTEZIONE E I FONDAMENTI DI LICEITA' DEL TRATTAMENTO

Il trattamento dei dati personali operato dal Comune di Oristano si fonda sulla liceità del trattamento e pertanto Tratta i dati solo se e nella misura in cui ricorre **almeno una delle seguenti condizioni:**

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

In particolare:

- per i dati "sensibili" il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati, compresa la profilazione;

- non deve essere necessariamente "documentato per iscritto", ne' è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilita' del consenso e il suo essere "esplicito" (per i dati sensibili) e a dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento;

- il consenso dei minori è valido a partire dai 16 anni fermo restando che il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale; prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci;

- deve essere, in tutti i casi, libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto (no a caselle prespuntate su un modulo)

- deve essere manifestato attraverso "dichiarazione o azione positiva inequivocabile".

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Il SISTEMA DI PROTEZIONE E L'INFORMATIVA

Nellôinformativa fornita dal Comune di Oristano sono contenuti:

- i dati di contatto del RPD;
- la base giuridica del trattamento;
- il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento;
- se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione;
- il diritto di presentare un reclamo allôautorità di controllo.

Informativa

Nel caso di dati personali non raccolti direttamente presso l'interessato l'informativa è fornita entro un termine ragionevole che non sia superiore a un mese dalla raccolta, oppure al momento della comunicazione (NON della registrazione) dei dati (a terzi o all'interessato).

Modalita' dell'informativa

L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile. Occorre utilizzare un linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee. Essa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico soprattutto nel contesto di servizi online anche se sono ammessi "altri mezzi", potendo essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra.

L'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati.

In caso di dati personali raccolti da fonti diverse dall'interessato, lôEnte valuta caso per caso se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato.

Se i dati non sono raccolti direttamente presso l'interessato, l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento.

In tutti i casi, il titolare deve specificare:

- la propria identità;
- quella dell'eventuale rappresentante nel territorio italiano;
- le finalità del trattamento;
- i diritti degli interessati (compreso il diritto alla portabilità dei dati);
- se esiste un responsabile del trattamento e la sua identità;
- quali sono i destinatari dei dati.

Ogni volta che le finalità cambiano è necessario informarne l'interessato prima di procedere al trattamento ulteriore.

Il SISTEMA DI PROTEZIONE E I DIRITTI DEGLI INTERESSATI

Modalita' per l'esercizio dei diritti

Il titolare del trattamento agevola l'esercizio dei diritti da parte dell'interessato, adottando ogni misura tecnica e organizzativa a ciò idonea. Benché' sia il solo titolare a dover dare riscontro in caso di esercizio dei diritti, il responsabile è tenuto a collaborare con il titolare o un suo delegato ai fini dell'esercizio dei diritti degli interessati. Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee. Sono ammesse deroghe ai diritti riconosciuti dal GDPR, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché' di altri articoli relativi ad ambiti specifici.
Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso) 1 mese, estendibili fino a 3 mesi in casi di particolare complessità; il titolare o un suo delegato deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano lôaccessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Diritto di accesso

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto di accesso secondo la quale l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo a unôautorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 GDPR, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché' l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia di cui al paragrafo 3 dell'art. 15 GDPR non deve ledere i diritti e le libertà altrui.

Diritto alla rettifica e cancellazione

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto di rettifica e cancellazione ("diritto all'oblio"), e di seguito indicata.

Quanto al diritto di rettifica, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Quanto al diritto cosiddetto "all'oblio", l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione;

Diritto alla limitazione

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto alla limitazione e di seguito indicata.
L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti condizioni:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché' il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del GDPR, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Diritto alla portabilita'

Il presente PPD tiene conto della disciplina del GDPR in tema di diritto alla portabilita' dei dati, e di seguito indicata.

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b);

b) il trattamento sia effettuato con mezzi automatizzati.

Il diritto alla portabilita' non deve ledere i diritti e le libertà altrui.

PARTE III

CONTESTO, SOGGETTI RESPONSABILI , SICUREZZA E DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE

IL CONTESTO DEL SISTEMA DI PROTEZIONE

La descrizione riassuntiva del contesto, tenendo conto della sintetica descrizione del trattamento e del flusso informativo, ha lo scopo di delineare il complessivo stato di fatto e di diritto nel quale si inserisce il trattamento, sia con riferimento al contesto esterno che con riferimento al contesto interno.
Per quanto concerne il contesto interno, tiene conto in particolare:

- degli atti di programmazione e pianificazione generale dell'Ente - disposizioni e atti generali (direttive, circolari, programmi e istruzioni) - organizzazione e articolazione degli uffici (organigramma) - mappatura dellôattività (processi e procedimenti) - inventario dei beni (mobili e immobili) e mappatura delle risorse strumentali - elenco di consulenti e collaboratori - atti e provvedimenti degli organi di indirizzo - catalogo di dati, metadati, banche dati - disciplina particolare dellôattività oggetto di trattamento;

- dei soggetti che effettuano il trattamento e dei soggetti che sono autorizzati ad accedere ai locali fuori dall'orario di servizio.

I SOGGETTI E LE RESPONSABILITA'

Titolare del trattamento

Il titolare è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui competono, anche unitamente ad altro titolare, le decisioni in ordine:

- alle finalità;
- alle modalità del trattamento di dati personali;

- agli strumenti utilizzati;
ivi compreso il profilo della sicurezza.

Le decisioni del titolare in ordine a quanto sopra tengono conto dei:

- principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari: il trattamento riguardante dati diversi da quelli sensibili e giudiziari è consentito soltanto per lo svolgimento delle funzioni istituzionali, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente. La comunicazione ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando e' comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2 D.Lgs. 196/2003, e non e' stata adottata la diversa determinazione ivi indicata. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento;

- principi applicabili al trattamento di dati sensibili: il trattamento dei dati sensibili è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, D.Lgs. 196/2003, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g) del decreto sopra citato, anche su schemi tipo. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2. L'identificazione dei tipi di dati e di operazioni è aggiornata e integrata periodicamente;

- principi applicabili al trattamento di dati giudiziari: il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili. Il trattamento dei dati giudiziari è altresì consentito quando è effettuato in attuazione di protocolli d'intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con i suoi uffici periferici di cui all'articolo 15, comma 2, del decreto legislativo 30 luglio 1999, n. 300, previo parere del Garante per la protezione dei dati personali, che specificano la tipologia dei dati trattati e delle operazioni eseguibili. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati giudiziari e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo. L'identificazione dei tipi di dati e di operazioni è aggiornata e integrata periodicamente;

- principi applicabili al trattamento di dati sensibili e giudiziari: il trattamento dei dati sensibili e giudiziari deve essere conformato secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato. Nel fornire l'informativa occorre fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari. E' possibile trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato. E' necessario verificare,

periodicamente, l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché' la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti attribuiti, e' necessario valutare specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione e' prestata per la verifica dellôindispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi e' autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità sopra indicate anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici. I dati idonei a rivelare lo stato di salute non possono essere diffusi. Rispetto ai dati sensibili e giudiziari indispensabili, è lecito effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psicoattitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché' i trattamenti di dati sensibili e giudiziari per la definizione di profili e della personalità dell'interessato, sono effettuati solo previa annotazione scritta dei motivi. In ogni caso, le operazioni e i trattamenti di cui ai test psicoattitudinali volti a definire il profilo o la personalità dell'interessato, se effettuati utilizzando banche di dati di diversi titolari, nonché' la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

Contitolari del trattamento

Allorché' due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.
I contitolari determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente GDPR, con particolare riguardo:

- all'esercizio dei diritti dell'interessato;

- alle rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR, 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 deve designare un punto di contatto dei contitolari per gli interessati. L'accordo riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato. Indipendentemente dalle disposizioni dell'accordo, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Responsabili del trattamento e sub-responsabili

Il Responsabile del trattamento è la persona fisica o giuridica, lôautorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Per effetto di tale modifica, il responsabile è il soggetto esterno alla struttura organizzativa che agisce "per conto del titolare".

Il responsabile è designato dal titolare facoltativamente. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti. In particolare, il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il responsabile effettua il trattamento attenendosi alle condizioni stabilite nel contratto o atto giuridico, e alle istruzioni impartite dal titolare, il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di legge e regolamento, delle proprie istruzioni e di quanto stabilito nel contratto o atto giuridico.
Ciò premesso in via generale in materia di responsabili del trattamento, per quanto concerne i fornitori di servizi di comunicazione elettronica accessibili al pubblico si rinvia integralmente alla disciplina degli artt. 32 e 32-bis del D.Lgs. n. 196/2003 anche per quanto concerne gli adempimenti conseguenti ad una violazione di dati personali

Incaricati

Pur non prevedendo espressamente la figura dellôòincaricato" del trattamento (ex art. 30 Codice), il GDPR non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto lôautorità diretta del titolare o del responsabile".

Restano applicabili le disposizioni del D.Lgs. n. 196/20013 in tema di incaricati. In particolare:

- le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorita' del titolare o del responsabile, attenendosi alle istruzioni impartite;

- la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti allôunità medesima.

Responsabile della protezione dei dati (RPD/DPO)

Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.

Il RPD/DPO:

- può svolgere altri compiti e funzioni a condizione che tali compiti e funzioni non diano adito a un conflitto di interessi;

- è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il responsabile della protezione dei dati è incaricato dei seguenti compiti:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché' ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente GDPR nonché' da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

- sorvegliare l'osservanza del presente GDPR, 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;

- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del DGPR;

- cooperare con lôautorità di controllo;

- fungere da punto di contatto per lôautorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti, il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il responsabile della protezione dei dati:

- va tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

- va sostenuto nell'esecuzione dei propri compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;

- non deve ricevere alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti.

Il responsabile della protezione dei dati non e' rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti.

Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

LA SICUREZZA

Misure di sicurezza

Fermo restando il principio che qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali e che, salvo quanto previsto dalla legge per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, **i soggetti pubblici non devono richiedere il consenso dell'interessato,** i trattamenti in ambito pubblico devono svolgersi in modo lecito e garantendo la sicurezza. A tal fine, il GDPR stabilisce che il titolare del trattamento attui misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto GDPR, tenendo conto tra l'altro dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1) . L'obbligo per il titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi.

Tenendo conto dello stato dell'arte e dei costi di adeguamento, nonché' della natura, dell'oggetto, 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, lôintegrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti 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.

Notifica di una violazione dei dati personali all'Autorita' di controllo

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione allôautorità di controllo competente a norma dell'articolo 55 del GDPR:
- senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica allôautorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

La notifica:

a) descrive la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché' le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunica il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) descrive le probabili conseguenze della violazione dei dati personali;

d) descrive le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Comunicazione di una violazione dei dati personali all'interessato

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato descrive, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR:

- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

- descrizione delle probabili conseguenze della violazione dei dati personali;

- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non si procede alla comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

LA DOCUMENTAZIONE DEL SISTEMA DI PROTEZIONE

Le diverse componenti del sistema di protezione sono documentati da:

- Piano protezione dati -PPD;
- Registri delle attività e delle categorie dei trattamenti;
- Mappa struttura organizzativa;
- Mappa dei soggetti;
- Mappa dei luoghi;
- Schede di ricognizione dei trattamenti/Indice-Mappa dei trattamenti;
- Mappa hardware;
- Mappa software;
- Mappa rischi e motivazioni stima;
- Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679/ Schede di assoggettabilità a DPIA;
- Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente;
- Mappa delle misure di sicurezza logistiche/fisiche;
- Mappa delle misure di sicurezza informatiche/logiche;
- Mappa delle misure di sicurezza organizzative;
- Mappa delle misure di sicurezza e procedurali;
- Elenco delle misure di sicurezza correlate all'indice dei trattamenti e suddivise per uffici.

PARTE IV

GESTIONE DEL RISCHIO

ai fini della strategia di protezione dei dati personali, viene definita:

- la nozione di "rischio" come uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.

- la nozione di "gestione dei rischi" come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta tenendo presente i seguenti principi:

a) La gestione del rischio crea e protegge il valore. La gestione del rischio contribuisce in maniera dimostrabile al raggiungimento degli obiettivi ed al miglioramento della prestazione, per esempio in termini di salute e sicurezza delle persone, security, rispetto dei requisiti cogenti, consenso presso l'opinione pubblica, protezione dell'ambiente, qualità del prodotto gestione dei progetti, efficienza nelle operazioni, governance e reputazione.

b) La gestione del rischio è parte integrante di tutti i processi dell'organizzazione. La gestione del rischio non è un'attività indipendente, separata dalle attività e dai processi principali dell'organizzazione. La gestione del rischio fa parte delle responsabilità della direzione ed e' parte integrante di tutti i processi dell'organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei progetti e del cambiamento.

c) La gestione del rischio è parte del processo decisionale. La gestione del rischio aiuta i responsabili delle decisioni ad effettuare scelte consapevoli, determinare la scala di priorità delle azioni e distinguere tra linee di azione alternative.

d) La gestione del rischio tratta esplicitamente l'incertezza. La gestione del rischio tiene conto esplicitamente dell'incertezza, della natura di tale incertezza e di come può essere affrontata.

e) La gestione del rischio è sistematica, strutturata e tempestiva. Un approccio sistematico, tempestivo e strutturato alla gestione del rischio contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili.

f) La gestione del rischio si basa sulle migliori informazioni disponibili.

g) La gestione del rischio è "su misura". La gestione del rischio è in linea con il contesto ~~esterno ed~~ interno e con il profilo di rischio dell'organizzazione.

j) La gestione del rischio è dinamica. La gestione del rischio è sensibile e risponde al cambiamento continuamente. Ogni qual volta accadono eventi esterni ed interni, cambiano il contesto e la conoscenza, si attuano il monitoraggio ed il riesame, emergono nuovi rischi, alcuni rischi si modificano ed altri scompaiono.

k) La gestione del rischio favorisce il miglioramento continuo dell'organizzazione. Le organizzazioni dovrebbero sviluppare ed attuare strategie per migliorare la maturità della propria gestione del rischio insieme a tutti gli altri aspetti della propria organizzazione.

La gestione di rischi derivanti dal trattamento sulla protezione dei dati personali viene condotta attraverso le fasi di:

- analisi del rischio, quale fase del processo di gestione nella quale viene definito il contesto esterno e interno, di natura organizzativa e gestionale;

- valutazione del rischio, quale fase del processo di gestione del rischio che identifica, analizza e pondera il rischio medesimo;

- trattamento del rischio.

GESTIONE DEL RISCHIO: FASE DELLA ANALISI

Contesto interno organizzativo

L'articolo 35 del GDPR fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche". Il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.
I documenti allegati e, in particolare, la ricognizione dei trattamenti in rapporto a tutta lôattività dell'ente, le schede di DPIA e l'elenco dei rischi, della gravità rilevata dalla prospettiva degli interessati e della relativa motivazione comprovano l'effettuazione della analisi dei rischi derivanti dai trattamenti, e l'accuratezza della analisi medesima.

1) MAPPA DELLA STRUTTURA ORGANIZZATIVA

La struttura organizzativa dell'Ente e' indicata nella MAPPA DELLA STRUTTURA ORGANIZZATIVA allegata, e corrisponde alle funzioni.

2) MAPPA DEI LUOGHI

La mappa dei luoghi è allegata, al presente piano e indica:

- la sede principale, con l'indicazione degli Uffici e la relativa descrizione;

- le sedi secondarie, con l'indicazione degli Uffici e la relativa descrizione.

3) MAPPA DEI SOGGETTI

Eô allegata al presente documento, riepiloga, con riferimento a tutti i trattamenti effettuati dall'Ente, i soggetti destinatari di compiti e funzioni in materia di trattamento dei dati personali allôinterno dellôEnte.

4) SCHEDE DI RICOGNIZIONE DEI TRATTAMENTI

Fanno parte del sistema di protezione le Schede di ricognizione dei trattamenti elaborate con riferimento a tutta lôattività svolta dall'Ente, prendendo in considerazione tutti i processi, inclusi i procedimenti amministrativi.

5) MAPPA HARDWARE

La Mappa hardware, allegata al presente documento per formarne parte integrante e sostanziale, identifica gli strumenti, i tipi di supporto e i locali di ubicazione. Fornisce, altresì, una descrizione delle caratteristiche tecniche degli strumenti elettronici medesimi.

6) MAPPA SOFTWARE

La Mappa software, allegata al presente documento per formarne parte integrante e sostanziale, identifica i software in relazione agli archivi/banche dati che vengono gestiti dai software medesimi.

Identifica, altresì, i soggetti abilitati all'accesso.

7) MAPPA DEI RISCHI

La Mappa dei rischi, allegata al presente documento per formarne parte integrante sostanziale, costituisce un elenco dei principali eventi rischiosi che possono determinare la violazione dei dati e rileva, dalla prospettiva degli interessati, la gravità e la correlata motivazione.

8) SCHEDE DI DETERMINAZIONE PRELIMINARE DELLA POSSIBILITA' CHE IL TRATTAMENTO "POSSA PRESENTARE UN RISCHIO ELEVATO" AI FINI DEL GDPR (UE) 2016/679

Fanno parte del sistema di protezione le Schede di determinazione preliminare della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del GDPR (UE) 2016/679, le quali vengono allegate al presente documento per formarne parte integrante sostanziale.

9) SCHEDE DI SINTESI DELLA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) PER LA PUBBLICAZIONE

Fanno parte del sistema di protezione le Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente.

10) MAPPA MISURE DI SICUREZZA LOGISTICHE/FISICHE

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza logistiche/fisiche.

11) MAPPA MISURE DI SICUREZZA INFORMATICHE/LOGICHE

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza informatiche/logiche.

12) MAPPA MISURE DI SICUREZZA ORGANIZZATIVE

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza organizzative.

13) MAPPA MISURE DI SICUREZZA PROCEDURALI

Fa parte integrante e sostanziale del sistema di protezione l'allegata MAPPA delle misure di sicurezza procedurali.

14) ELENCO MISURE DI SICUREZZA

Fa parte integrante e sostanziale del sistema di protezione l'allegato ELENCO misure di sicurezza, correlate alla ricognizione/indice dei trattamenti e suddivise per uffici.

15) REGISTRO DELLE ATTIVITA' DI TRATTAMENTO E DELLE CATEGORIE DI ATTIVITA'

Fanno parte integrante sostanziale del sistema di protezione:

- il Registro delle attività di trattamento svolte sotto la responsabilità del titolare;

Altri documenti del Sistema di protezione

Costituiscono parte del sistema di protezione, per formarne parte integrante sostanziale:

- atti di delega al trattamento dei dati;

- atti di nomina degli incaricati.

Costituiscono parte del sistema di protezione, quand'anche non fisicamente allegati al presente documento, i seguenti ulteriori documenti:

- codice di condotta dell'Ente;
- piano di formazione in materia di diritti e di libertà delle persone e di protezione dei dati personali per i soggetti autorizzati al trattamento e per incaricati del back up;
- contratti/clausole contrattuali con i responsabili del trattamento;
- circolari;
- informazioni fornite al pubblico e agli interessati;
- altra documentazione utile a comprovare la conformità dei trattamenti al GDPR e alla normativa interna di adeguamento.

PARTE V

GESTIONE DEL RISCHIO FASE DELLA VALUTAZIONE

Determinazione di assoggettabilità dei trattamenti a valutazione di impatto ï DPIA

La valutazione del rischio richiede l'identificazione, l'analisi e la ponderazione del rischio medesimo.
Ai fini della valutazione del rischio è necessario procedere a una valutazione d'impatto del trattamento sulla protezione dei dati.
La valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché' a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli.
Cio' premesso, il presente PPD tiene presente, in via generale, che:

- qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità;

e' necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento "possa presentare un rischio elevato", intendendosi per "rischio" uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità, e per "gestione dei rischi" l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi;

- la valutazione d'impatto sulla protezione dei dati va effettuata anche per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, o, ad esempio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento;

- la valutazione d'impatto sulla protezione dei dati può riguardare una singola operazione di trattamento dei dati. Tuttavia vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto. Pertanto si può ricorrere a una singola valutazione d'impatto sulla protezione dei dati nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. In effetti, le valutazioni d'impatto sulla protezione dei dati mirano a studiare sistematicamente nuove situazioni che potrebbero portare a rischi elevati per i diritti e le libertà delle persone fisiche e non è necessario realizzare una valutazione d'impatto sulla protezione dei dati nei casi (ad esempio operazioni di trattamento in un contesto specifico e per una finalità specifica) che sono già stati studiati;

- la valutazione d'impatto va effettuata applicando le Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679;

- l'esito della valutazione va preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il GDPR. In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

Determinazione di assoggettabilità dei trattamenti a valutazione di impatto - DPIA

Preliminare per la valutazione di impatto è la determinazione del titolare in ordine alla possibilità che il trattamento possa determinare un rischio elevato per i diritti e le libertà degli interessati.

La decisione in ordine alla possibilità che il trattamento in epigrafe indicato possa produrre un rischio elevato sulla protezione dei dati delle persone fisiche e, quindi, sulla obbligatorietà della DPIA viene adottata applicando i 3 casi indicati l'art. 35, paragrafo 3 del GDPR e i 9 CRITERI esplicativi contenuti nelle "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679" adottate dal Garante il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 (di seguito solo "Linee guida").

Nell'applicare i suddetti CRITERI si è tenuto conto di quanto segue:

- la DPIA è sempre obbligatoria, indipendentemente dalla presenza di uno o più criteri sopra menzionati, per tutti i trattamenti inclusi nell'elenco predisposto e pubblicato dallôAutorità di controllo ai sensi dell'art. 35, paragrafo 4 GDPR;

- la DPIA è sempre obbligatoria per i trattamenti inclusi nell'indice dei trattamenti dei dati sensibili e giudiziari ai sensi del Regolamento sul trattamento dei dati sensibili e giudiziari approvato dall'Ente conformemente allo schema tipo del Garante;

- fermo restando che, secondo le Linee guida, un trattamento che soddisfa 2 criteri deve formare oggetto di una valutazione d'impatto sulla protezione dei dati, tuttavia, al fine di garantire una maggiore garanzia di tutela, la ricorrenza anche di 1 solo criterio costituisce elemento sufficiente per originare l'obbligo di svolgimento della DPIA;

- maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati;

- se, pur applicando i criteri sopra indicati, la necessità di una DPIA non emerge con chiarezza, va comunque ritenuto sussistente l'obbligo - secondo quanto raccomandato dal WP29 - di farvi ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento;

- la valutazione d'impatto sulla protezione dei dati non è richiesta nei seguenti casi:

- quando, sulla base di predetti criteri, risulta che il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche ";

- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo;

- quando le tipologie di trattamento sono state verificate da unôautorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate;

- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e) GPDR, trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia gia' stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10 GPDR).

In ordine ai diversi trattamenti, le SCHEDE allegate per formare parte integrante e sostanziale del presente PPD, evidenziano le determinazioni assunte, tenendo conto delle linee guida adottate in materia.

Valutazione di impatto - DPIA per trattamenti a rischio elevato
In base alle determinazioni di assoggettabilità a valutazione di impatto di cui alle allegate SCHEDE (DPIA-FASE 1), i trattamenti per i quali risulta determinato, un elevato rischio per i diritti e le libertà delle persone fisiche, e che non rientrano tra le eccezioni sono assoggettati a valutazione di impatto (DPIA-FASE 2).

Per tali trattamenti:

- la determinazione sulla possibilità di un rischio elevato risulta documentata in atti (SCHEDE DPIA - FASE 1) dalle SCHEDE aventi funzione di RELAZIONE/REPORT;

- lo svolgimento della DPIA viene condotto secondo lo schema di flusso desunto dalle Linee guida in precedenza citate ed è documentato e comprovato in atti (SCHEDE DPIA - FASE 2)

Il GDPR non definisce formalmente il concetto di valutazione d'impatto sulla protezione dei dati come tale, tuttavia il suo contenuto minimo è specificato dall'articolo 35, paragrafo 7 GDPR, come segue:

"a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione".

In ordine ai diversi trattamenti, e sulla base determinazioni assunte in ordine alla possibilità che il trattamento possa comportare un rischio elevato per i diritti e le libertà degli interessati, le valutazioni di impatto documentate dalle SCHEDE (DPIA- FASE 2) sono state effettuate tenendo presente i ruoli stabiliti nelle Linee guida.

Pubblicazione sintesi della valutazione d'impatto ï DPIA

La pubblicazione della valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal GDPR generale sulla protezione dei dati, è una decisione del titolari del trattamento procedere in tal senso.

Tuttavia, il Comune di Oristano ha pubblicato della valutazione d'impatto sulla protezione dei dati e reperibili al seguente link:

PARTE VI

GESTIONE DEL RISCHIO: FASE DEL TRATTAMENTO

Misure di sicurezza del trattamento

Il GDPR prevede che il titolare del trattamento attui misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto GDPR, tenendo conto tra l'altro dei "rischi aventi probabilita' e gravita' diverse per i diritti e le liberta' delle persone fisiche" (articolo 24, paragrafo 1). L'obbligo per il titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi.

Misure di sicurezza logistiche/fisiche

Sicurezza di aree e locali

L'identificazione delle misure di sicurezza logistiche/fisiche ha tenuto conto dei sotto indicati elementi di rischio, indicati a titolo esemplificativo e non esaustivo:

a) Vicinanza servizi
- Carabinieri o altre forze di polizia e vigilanza
- Ospedali o altri presidi
- Vigili del fuoco

b) Misure presenti anti intrusione
- Antifurto
- Vigilanza
- Videosorveglianza
- Controllo accessi
- Recinzioni
- Cancelli

c) Misure presenti anti incendio
- Estintori

d) Misure presenti per la regolarità degli impianti
- Elettrico
- Climatizzazione
- Riscaldamento

e) Misure presenti per la continuità elettrica
- UPS (pari al 50% delle postazioni di lavoro)

f) Procedure
- Procedura di gestione degli accessi

L'identificazione delle misure di sicurezza logistiche/fisiche ha preso in considerazione le principali sotto indicate misure, elencate a titolo esemplificativo e non esaustivo:

a) antifurto
- Allarmi
- Videosorveglianza
- Porta normale
- Serratura di sicurezza
- Finestre con grate
- Finestre senza grate

b) antincendio
- Estintori

d) Sicurezza accessi
- Controllo
- Altro
e) Sicurezza CED
- Controllo accessi
- Impianto di climatizzazione
- Misure antincendio (estintori) idonee all'uso con le apparecchiature presenti

f) continuita' operativa
- Gruppo di continuita'
- Corretto ed ordinato posizionamento dei cavi elettrici
- Corretto ed ordinato posizionamento dei cavi di rete
- Posizionamento ordinato delle apparecchiature nei rack
- Spazio intorno ai rack adeguato per la movimentazione e manutenzione delle apparecchiature

g) Sistema di custodia archivi cartacei
- Altri armadi con serratura
- Altri armadi senza serratura
- Classificatori/cassetti con serratura
- Classificatori/cassetti senza serratura
- Cassaforte
- Scaffalature

La MAPPA delle misure di sicurezza logistiche/fisiche applicate ai diversi trattamenti, allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Misure di sicurezza informatiche/logiche

Al fine di indicare alle pubbliche amministrazioni le misure minime per la sicurezza ICT che debbono essere adottate per contrastare le minacce piu' comuni e frequenti cui sono soggetti i loro sistemi informativi, ed in adeguamento della Direttiva 1 agosto 2015 del Presidente del Consiglio dei Ministri che emana disposizioni finalizzate a consolidare lo stato della sicurezza informatica nazionale, AgID ha provveduto ad emanare l'elenco ufficiale delle "Misure minime per la sicurezza ICT delle pubbliche amministrazioni".
Con l'avvenuta pubblicazione in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017) della Circolare 18 aprile 2017, n. 2/2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1 agosto 2015)", le Misure minime sono ora divenute di obbligatoria adozione per tutte le Amministrazioni.

Per l'identificazione delle misure minime informatiche/logiche, per la sicurezza ICT ai fini del presente PPD si rinvia alle suddette misure minime per la sicurezza ICT delle pubbliche amministrazioni come attuate e implementate dal titolare.

La MAPPA delle misure di sicurezza informatiche/logiche applicate ai diversi trattamenti inclusi i criteri e modalita' di salvataggio e di ripristino della disponibilita' dei dati, allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Misure di sicurezza organizzative

A titolo esemplificativo e non esaustivo, si elencano le seguenti misure minime:

- individuazione dell'ambito del trattamento consentito ai singoli incaricati
- istruzioni da impartire agli incaricati medesimi

- controllo, custodia e restituzione della documentazione
- controllo degli accessi degli archivi/banche dati";
- misure organizzative per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, lôintelligibilità e la completezza del riscontro fornito agli interessati";
- formazione di tutti i soggetti che trattano dati personali sotto lôautorità del titolare e del responsabile del trattamento, e divieto di trattamento dei dati personali senza previa istruzione in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'unione o degli stati membri;
- distruzione documenti non necessari
- misure organizzative necessarie a documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché' necessarie a documentare le procedure effettuate per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi secondo le prescrizioni del garante";
- separazione documenti e dati;
- informazione continua e aggiornamento costante su procedure operative e istruzioni;
- prescrizioni nellôattività di videosorveglianza prescrizione del rispetto di tutte le misure e gli accorgimenti prescritti autorità Garante come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello";
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- integrazione della gestione del rischio di violazione di sicurezza dei dati personali in tutti i processi/procedimenti";
- integrazione, nella gestione dei processi, delle procedure e istruzioni operative sulla sicurezza del trattamento e riunioni periodiche sul tema della sicurezza del trattamento.

La MAPPA delle misure di sicurezza organizzative, applicate ai diversi trattamenti allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Misure di sicurezza procedurali

Le misure di sicurezza procedurali sono identificate in base ai contenuti e indicazioni del GDPR.

A titolo esemplificativo e non esaustivo, si elencano:

- definizione procedura operativa per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati garantendo, in particolare, l'intelligibilita' e la completezza del riscontro fornito agli interessati";

- definizione procedura operativa per gestire le violazioni della sicurezza dei dati (data breach) secondo le prescrizioni del Garante";

- definizione procedura operativa per il ripristino tempestivo della disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico";

- definizione procedura operativa per la pseudonimizzazione e cifratura dei dati personali";

- definizione e attuazione procedura operativa per la conservazione di determinati atti in archivi ad accesso ristretto;

- definizione procedura operativa per testare, verificare e valutare regolarmente l'efficacia:

a) delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

b) le misure di ripristino in caso di "data breach";

- definizione e attuazione procedure operative per assicurare, con riferimento alle misure previste dal disciplinare tecnico allegato B al D.Lgs. 196/2003 per i trattamenti con strumenti diversi da quelli elettronici:

a) l'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
b) le modalita' e i contenuti delle istruzioni da impartire agli incaricati medesimi;
c) le modalita' del controllo, custodia e restituzione della documentazione;
d) le modalita' del controllo degli accessi agli archivi/banche dati";
- definizione e attuazione procedura operativa per documentare eventuali violazioni dei dati personali, comprese le circostanze a essa relative e le sue conseguenze, nonche' per documentare i provvedimenti adottati per porvi rimedio nonche' per gestire le violazioni della sicurezza dei dati (data breach) e il ripristino degli stessi";

- definizione e attuazione procedura operativa per selezionare e formare i soggetti inserire nel Piano formativo avente ad oggetto: a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali b) Formazione di base di primo livello di natura tecnica sul processo di gestione del rischio ai sensi della norma UNI ISO 31000 e del GDPR".

La MAPPA delle misure di sicurezza procedurali, applicate ai diversi trattamenti e' allegata al presente PPD per formarne parte integrante e sostanziale, documenta e comprova l'osservanza del GDPR.

Piano formativo

Il piano formativo deve essere impostato sulla base dei seguenti CRITERI:

a) Formazione di base di primo livello di natura giuridica avente ad oggetto i diritti e le liberta' delle persone fisiche e sulla protezione di tali diritti e liberta', con particolare riferimento al diritto alla protezione dei dati personali;

ALLEGATI

Mappa struttura organizzativa

Mappa dei soggetti del sistema di protezione, inclusi i soggetti esterni cui e' affidato il trattamento dei dati

Mappa dei trattamenti
Mappa dei luoghi
Mappa hardware
Mappa rischi in formato digitale
Link Schede di sintesi della valutazione di impatto sulla protezione dei dati (DPIA) da pubblicare sul sito web dell'Ente
Mappa delle misure di sicurezza logistiche/fisiche
Mappa delle misure di sicurezza informatiche/ logiche
Mappa delle misure di sicurezza organizzative
Mappa delle misure di sicurezza procedurali
Link Atti di delega al trattamento dei dati