

01. ACQUISIZIONE DI DATI PERSONALI

Gestione di procedure relative al rapporto di lavoro

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
L'acquisizione di dati personali, sia in forma cartacea che informatizzata, deve avvenire nel rispetto dei principi di: - competenza: la persona che acquisisce le informazioni deve essere autorizzata o rivestire un ruolo da cui discende la legittimità dell'acquisizione - minimizzazione: le informazioni che vengono acquisite debbono essere strettamente limitate all'espletamento delle procedure per le quali sono richieste - informazione: i soggetti a cui si riferiscono i dati debbono essere informati in modo completo e adeguato riguardo alle motivazioni che richiedono l'acquisizione delle informazioni, oltre che sulle modalità di utilizzo e di esercizio dei propri diritti - responsabilizzazione: ogni operatore che acquisisce informazioni e dati personali è tenuto ad assicurarsi della loro corretta conservazione e destinazione, nel rispetto delle prescrizioni procedurali.	il trattamento a cui si fa riferimento riguarda l'acquisizione di dati all'interno dell'ente	- acquisizione di dati e informazioni da parte di un soggetto non autorizzato - acquisizione di informazioni ridondanti e non strettamente funzionali alle procedure che hanno determinato la richiesta - errore nella destinazione dei dati o delle informazioni acquisite che può causare la perdita del dato o la indebita divulgazione	- nomina degli "incaricati del trattamento" ai fini della individuazione degli operatori abilitati all'acquisizione dei dati e della informazioni - definizione delle procedure di acquisizione dei dati e delle informazioni anche riguardo alla destinazione dei dati - predisposizione di informative che consentano agli interessati di acquisire informazioni riguardo alla base giuridica che prescrive il trattamento e alle modalità di gestione e conservazione dei dati, oltre ai contatti relativi al titolare e al responsabile e alle modalità di esercizio dei propri diritti.

02. CONSERVAZIONE DI DATI IN FORMATO CARTACEO

Attività finalizzate alla conservazione e all'archiviazione di atti e dati

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
I documenti debbono essere conservati all'interno dei fascicoli relativi alle pratiche di cui fanno parte, in modo da potere essere facilmente reperiti quando necessario. Debbono essere conservati in luoghi che non siano esposti a intemperie o a rischi di incendio o a eventuali possibilità di altre forme di deterioramento. debbono essere riposti in contenitori o mobili il cui accesso sia limitato agli operatori e incaricati del trattamento ed escluso a persone estranee, anche mediante l'utilizzo di chiavi fisiche o altri accorgimenti che garantiscano la sicurezza della corretta conservazione	La conservazione dei documenti cartacei può essere affidata a soggetti esterni a condizione che ciò avvenga a seguito di un incarico formale e che siano definite le modalità di conservazione e le relative responsabilità.	Perdita o distruzione di documenti	- predisposizione del manuale della conservazione - definizione della modalità di conservazione dei dati e dei documenti - verifica periodica dell'integrità degli atti depositati

03. CONSERVAZIONE DI DATI IN FORMATO DIGITALE

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
I dati e di documenti debbono essere depositati in archivi che forniscano le garanzie di sicurezza prescritte dalle disposizioni in materia di sicurezza informatica. L'accesso agli archivi deve essere consentito esclusivamente a chi sia autorizzato e deve essere rilevato e registrato affinché ne rimanga traccia anche riguardo a eventuali modifiche e rimozione dei dati.	La conservazione dei documenti informatizzati può essere affidata a soggetti esterni a condizione che ciò avvenga a seguito di un incarico formale e che siano definite le modalità di conservazione e le relative responsabilità.	Perdita o distruzione di documenti, nonché eventuali minacce che impediscano l'accesso o ne compromettano l'integrità.	- predisposizione del manuale della conservazione - definizione della modalità di conservazione dei dati e dei documenti

04. GESTIONE DI DATI MEDIANTE L'UTILIZZO DI SISTEMI INFORMATIZZATI

Acquisizione, elaborazione, riproduzione, trasmissione, conservazione e trasmissione di dati mediante sistemi automatizzati per la gestione digitale delle informazioni

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
- inserimento di dati da parte di operatori dell'Ente o acquisizione da fonti esterne, elaborazioni, produzione e trasmissione di documenti - l'accesso ai sistemi informatizzati è consentito esclusivamente ai soggetti che siano espressamente autorizzati, con la prescrizione delle attività che possono svolgere e dei dati che possono conservare. - ai fini dell'accesso si provvede a rilasciare credenziali personali con l'obbligo di provvedere all'aggiornamento periodico - nel caso in cui l'accesso sia autorizzato a soggetti esterni dovranno essere definite formalmente le modalità e i tempi di accesso precisandone criteri e responsabilità	- Alcune fasi della procedura possono essere gestite mediante l'utilizzo di applicativi gestionali di proprietà di soggetti esterni - La conservazione dei dati può essere effettuata mediante l'utilizzo di server esterni (cloud) di proprietà di operatori esterni all'Ente	- accesso indebito al sistema informatico - utilizzo indebito dei dati da parte di operatore autorizzato all'accesso - trasmissione di dati e informazioni a destinatario errato o non autorizzato - compromissione dell'integrità dei dati conservati	- individuazione e definizione formale dei profili di accesso al sistema - definizione di una procedura per la gestione degli account e delle password - verifiche periodiche del registro degli accessi e degli utilizzi del sistema

05. ACCESSO AGLI ATTI

Autorizzazione alla visione o all'estrazione di copia a seguito di richiesta specifica

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
- l'accesso alla documentazione o ai dati detenuti dall'ente può essere consentito esclusivamente a seguito di una specifica richiesta, da parte di soggetti interessati, ai sensi delle disposizioni normative vigenti e nel rispetto delle modalità prescritte - la procedura per la visione o il rilascio di documenti deve rispettare le prescrizioni fornite dall'ente e viene esercitata esclusivamente dalle persone autorizzate - la visione o la copia dei documenti è strettamente riservata agli atti di cui si abbia diritto, provvedendo a oscurare eventuali informazioni che non siano ostensibili perché ridondanti o lesive della riservatezza - Prima dell'autorizzazione all'accesso, deve essere valutata l'eventuale pregiudizio per la riservatezza di terzi. Laddove ciò si verifici è necessario contattare i controinteressati e valutare eventuali violazioni prima di autorizzare la visione o la copia.	Non è previsto	- eventuali autorizzazione di documenti a soggetti che non abbiano titolo - eventuale ostensione di informazioni che si rivelano ridondanti o lesive della riservatezza di terzi	- definizione puntuale della procedura di accesso - verifica dell'interesse ad accedere - informazione al controinteressato e richiesta di trasmissione di eventuali situazioni ostative

06. TRATTAMENTO DI DATI RELATIVI A GIUDIZI O VALUTAZIONI

Gestione, elaborazione e conservazione di dati relativi a valutazioni e giudizi nei confronti di persone interne o esterne all'Ente

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
- L'acquisizione, l'elaborazione e la conservazione di dati che riguardano giudizi valutativi nei confronti di soggetti interni o esterni all'Ente deve essere gestita esclusivamente da persone specificamente incaricate. - Le informazioni potranno essere accessibili nelle forme e nelle modalità previste dalla normativa sull'accesso documentale.	L'Ente può avvalersi di un software di proprietà di un soggetto esterno con il quale vengono definiti gli ambiti e le modalità di utilizzo dei dati e le conseguenti responsabilità.	- Eventuale indebito accesso alla documentazione	- Limitazione dell'accesso ai soli operatori autorizzati - Conservazione in luogo sicuro e inaccessibile agli estranei o con sistemi di accreditamento.

07. TRATTAMENTO DI DATI PARTICOLARI E GIUDIZIARI

Acquisizione, elaborazione, conservazione, trasmissione e gestione di dati particolari e giudiziari

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
- Il trattamento dati particolari (religione, appartenenza politica, condizioni di salute, condizioni di indigenza) o giudiziari deve essere strettamente effettuato solo quando sia prescritto da specifiche norme di legge. - I dati particolari o giudiziari debbono essere trattati nel rispetto del principio di minimizzazione limitandone l'uso a esigenze comprovate e specifiche prescrizioni. - I dati particolari o giudiziari debbono essere trattati esclusivamente dal personale autorizzato e conservati in modo da assicurarne l'integrità e l'inaccessibilità a soggetti non autorizzati.	Non è previsto alcun ricorso a soggetti esterni	- Eventuale acquisizione di dati ridondanti - Eventuale indebito accesso alla documentazione - Eventuale indirizzamento delle informazioni a un destinatario errato	- Prescrizione delle procedure per l'acquisizione di dati particolari giudiziari - Limitazione dell'accesso esclusivamente al personale autorizzato - Registrazione degli accessi e delle attività svolte con l'utilizzo di dati particolari o giudiziari.

08. DIVULGAZIONE DEI DATI MEDIANTE LA PUBBLICAZIONE SUL SITO ISTITUZIONALE DELL'ENTE

Pubblicazione di informazioni e dati sul sito istituzionale dell'Ente

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
La pubblicazione di dati sul sito istituzionale è consentita esclusivamente nei casi in cui sia espressamente prevista da norme di Legge e nel rispetto dei tempi e delle modalità previste. L'Ente individua i soggetti autorizzati alla pubblicazione dei dati sul sito istituzionale assicurando che non siano divulgate informazioni che possano ledere la riservatezza o comunque violare i principi relativi al trattamento dei dati personali.	L'Ente può avvalersi di soggetti esterni a cui affidare la gestione delle pubblicazioni sul sito istituzionale	Eventuale pubblicazione di informazioni ridondanti e non pertinenti	- Individuazione dei soggetti responsabili della pubblicazione - Definizione della procedura relativa alla pubblicazione dei dati sul sito istituzionale - Effettuazione di audit periodici

09. ACQUISIZIONE DI SEGNALAZIONI DI ILLECITI

Acquisizione di informazioni, esposti, denunce, rilievo o segnalazioni sia da parte di interni che di esterni all'Ente

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
- L'acquisizione di segnalazioni, rimostranze o denunce deve essere effettuata esclusivamente da parte di soggetti espressamente autorizzati - I dati raccolti a tal fine debbono essere strettamente limitati alle finalità della segnalazione - I dati acquisiti debbono essere custoditi in modo da evitare assolutamente il rischio di un accesso indebito - I dati acquisiti debbono essere immediatamente trasmessi al soggetto o alle autorità competenti assicurando la massima riservatezza sul loro contenuto - I soggetti che presentano segnalazione debbono essere informati sulle modalità di trattamento dei dati	- L'Ente può affidare a soggetti esterni la gestione automatizzata delle segnalazioni	- Indebiti accesso e divulgazione delle informazioni acquisite - Eventuale indirizzamento delle informazioni a un destinatario errato	- Informazione al segnalante delle modalità di trattamento - Utilizzo di accorgimenti che garantiscano la riservatezza e l'integrità delle informazioni acquisite

10. APPLICAZIONE DI SANZIONI

Gestione di informazioni ai fini dell'istruttoria per l'applicazione di sanzioni

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
- L'Ente può applicare sanzioni esclusivamente nel rispetto del principio di legalità, cioè quando vi sia una specifica prescrizione normativa. - Al procedimento sanzionatorio possono partecipare esclusivamente i soggetti che siano espressamente autorizzati, con l'impegno di assicurare la massima riservatezza - La documentazione che viene acquisita dovrà essere conservata in modo da assicurarne l'integrità utilizzando ogni accortezza affinché non sia esposta al rischio di una indebita divulgazione - L'archivio contenente le sanzioni comminate deve essere depositato in luogo sicuro e con modalità che ne consentano l'accesso esclusivamente alle persone autorizzate	Non è previsto ricorso a soggetti esterni fatta eccezione per l'eventualità di archiviazione dei dati in cloud.	- Eventuale indebito accesso all'archivio - Eventuale indebita divulgazione - Eventuale indirizzamento delle informazioni a un destinatario errato	- Utilizzo di procedure che garantiscano il massimo della sicurezza - Accesso limitato ai soli operatori autorizzati

11. UTILIZZO DI SISTEMI DI GEOLOCALIZZAZIONE

Acquisizione e gestione di informazioni sulla localizzazione di autovetture o altri mezzi dell'ente

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
L'utilizzo di sistemi che possano rilevare la posizione di automezzi o strumenti in uso da parte del personale deve essere oggetto di informazione preventiva al fine di rendere edotto ogni operatore delle ragioni delle rilevazioni, delle modalità di trattamento delle informazioni e delle modalità per l'esercizio dei propri diritti. La gestione, acquisizione e conservazione di tali dati è consentita esclusivamente al personale autorizzato e limitatamente alle finalità istituzionali L'ente deve definire le modalità di acquisizione e i tempi e le modalità di conservazione.	laddove l'ente ricorra o soggetti esterni è necessario che definisca le modalità di espletamento del servizio e le rispettive responsabilità del trattamenti	- eventuale accesso indebito alle informazioni	- definizione della procedura di impiego dei dati - predisposizione di una informativa da fornire ai soggetti cge utilizzano direttamente o indirettamente i mezzi sottoposti a rilevazione

12. RIMOZIONE DI DATI PERSONALI

Attività consistente nella cancellazione definitiva di un dato all'interno di un archivio

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
La cancellazione di un dato personale deve essere effettuata nel rispetto delle seguenti modalità: - accertamento delle motivazioni che richiedono l'intervento di rimozione del dato - autorizzazione alla rimozione da parte del responsabile del trattamento, con specifico riferimento al dato da rimuovere o in via generale in relazione alle funzioni attribuite all'operatore che effettua la cancellazione - verifica che il dato cancellato possa essere eventualmente recuperato o in caso di cancellazione definitiva che non comporti danno all'interessato -	l'operazione di cancellazione avviene in modo diretto all'interno dell'ente	- eventuale rimozione errata di dati personali	- effettuazione di backup periodici - autorizzazione alla rimozione del dato - informazione dell'interessato nei casi in cui sia richiesta

13. INTERVENTI DI MODIFICA DI DATI PERSONALI

Operazioni finalizzate alla rimozione di dati dagli archivi dell'ente

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
Le attività dirette a modificare i dati personali conservati negli archivi dell'ente avvengono secondo le seguenti modalità: - le modifiche di dati già registrati nei database possono essere effettuate solo a seguito di richiesta motivata da parte dell'interessato, formalmente accolta o per il riscontro di un errore che si ritenga di dovere rettificare. In questo caso, se il dato errato è già stato oggetto di trattamento è necessario mantenere traccia dell'avvenuta modifica - le modifiche possono essere effettuate esclusivamente dagli operatori autorizzati all'accesso ai sistemi informatici nei quali il dato risiede	Non è previsto il ricorso a esterni	eventualità di un intervento di rettifica di un dato corretto	- registrazione delle modifiche effettuate quando riguardano dati che siano stati oggetti di precedente trattamento - autorizzazione alle modifiche esclusivamente agli operatori che hanno accesso ai sistemi informatici

14. TRATTAMENTO DI DOCUMENTI IDENTIFICATIVI

acquisizione, conservazione, consultazione e trasmissione di documenti identificativi

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
L'acquisizione di documenti identificativi è consentita esclusivamente nei casi in cui sia richiesta da norme di legge o regolamentari. In ogni caso i documenti identificativi non possono essere utilizzati al di fuori della procedura per cui sono stati acquisiti La trasmissione di documenti identificativi ad altri soggetti, sia interni che esterni, è limitata alle operazioni per le quali ciò sia necessario e previsto esplicitamente dalla procedura. Ogni trattamento che riguarda un documento identificativo deve essere tracciato, anche con un'annotazione, con l'indicazione dell'operatore che lo trasmette, delle ragioni della trasmissione, del destinatario e della data	Non è previsto il ricorso a esterni	eventualità di accesso indebito o trasmissione errata a soggetto non autorizzato all'acquisizione	- conservazione del documento in modalità sicura - registrazione di ogni trattamento

15. TRATTAMENTO DI DATI MEDIANTE UN'APPARECCHIATURA PERSONALE

Acquisizione, modifica, conservazione, elaborazione, consultazione e trasmissione di dati personali, per conto dell'ente, mediante apparecchiature personali

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
L'utilizzo di apparecchiature di proprietà personale è consentito nell'ambito delle prescrizioni contenute del Codice dell'amministrazione digitale adottato con il decreto legislativo 82/2005. In particolare è consentito l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti soggetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo. In caso di uso di dispositivi elettronici personali, viene adottata ogni misura atta a garantire la sicurezza e la protezione delle informazioni e dei dati, nonché a condizione che sia data al lavoratore adeguata informazione sull'uso sicuro dei dispositivi, anche attraverso la diffusione di apposite linee guida, e disciplinando, tra l'altro l'uso di webcam e microfoni, previa informazione alle organizzazioni sindacali.	non è previsto il ricorso a gestori esterni	eventualità che i dati personali di cittadini, operatori economici o altro soggetti vengano trattati da dipendenti con l'utilizzo di mezzi personali che non risultino protetti da eventuali accessi da parte dell'esterno	

16. ACCESSO ALL'ENTE A SOGGETTI ESTRANEI A SEGUITO DI ATTRIBUZIONE DI INCARICHI O AFFIDAMENTO DI SERVIZI

il trattamento riguarda i casi in cui l'ente consenta l'accesso ai locali e agli atti da parte di soggetti estranei a cui sia stato affidato un incarico di collaborazione o la gestione di un servizio

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
Nel caso in cui un soggetto estraneo all'ente sia incaricato di effettuare qualsiasi attività sia di tipo operativo che di concetto o di tipo istruttorio, questi, ai sensi dell'articolo 2, comma 2 del DPR 62/2013 - Codice di comportamento, deve essere messo al corrente degli obblighi comportamentali che gravano sia sui dipendenti pubblici, sia sui consulenti e collaboratori, sia sul personale delle imprese che operano all'interno dell'ente. I soggetti di cui sopra debbono essere messi al corrente dei trattamenti previsti nel registro del titolare, dei rischi connessi e delle misure previste. Debbono essere addestrati sull'uso corretto dei dati personali e sulle violazioni previste nel Regolamento generale per la protezione dei dati personali, oltre che sul Regolamento adottato dall'Ente. In ogni caso i soggetti debbono essere ammoniti sugli obblighi di segretezza e sul divieto di consultazione, accesso, copia e divulgazione di informazioni e dei	Il trattamento riguarda, in modo particolare il ricorso a soggetti esterni	- eventuale indebito accesso a dati o informazioni riservate - eventuale ingiustificata riproduzione o divulgazione di documenti - inadeguatezza delle modalità di conservazione dei dati	- Consegna del codice di comportamento - Consegna del registro del titolare con i trattamenti dell'ente - Consegna del Registro del trattamento relativo al settore di competenza - Assegnazione di compiti e funzioni con l'indicazione dei dati dei quali può effettuare il trattamento

17. ARCHIVIAZIONE DI DATI SU DISPOSITIVI MOBILI (CHIAVETTE USB - MICRO CARD SD -)

Archiviazione informatica di dati su supporti mobili

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
Esportazione di documenti, dati, informazioni ed elaborazioni su uno o più dispositivi di archiviazione esterni ai fini della conservazione, del trasporto dei dati o della trasmissione ad altro soggetto ecc. Tale trattamento deve avvenire nel rispetto dei seguenti principi: - responsabilizzazione: i dati possono essere trattati ed esportati esclusivamente da soggetti autorizzati al trattamento e nell'ambito delle funzioni di competenza, nell'esercizio di funzioni che ne consentano l'esportazione. - liceità: i dati possono essere esportati esclusivamente laddove ciò sia consentito da disposizioni normative o di carattere organizzativo; - sicurezza: l'esportazione del dato deve avvenire avendo cura di utilizzare strumenti che garantiscano l'assenza di eventuali	Ogni eventuale esportazione di dati su supporto mobile destinato o appartenente a soggetti esterni dovrà essere annotato e consentito esclusivamente nel caso in cui questi ultimi siano legittimati all'accesso o espressamente autorizzati.	- Eventuale trasferimento di informazioni ridondanti e non pertinenti; - Perdita del supporto di conservazione dei dati; - Deterioramento del supporto e impossibilità di accesso ai dati; - Accesso indebito alle informazioni da parte di un soggetto estraneo ed eventuale ulteriore riproduzione dei dati	- Limitazione della esportazione esclusivamente all'interno di procedure che la prevedano o per l'esercizio di funzioni che lo richiedano e limitatamente ai soli dati strettamente necessari; - Registrazione di ogni duplicazione ed esportazione di dati su supporti esterni non previsti dalle procedure di lavoro e trattamento; - Utilizzo di sistemi di sicurezza, sia fisici che logici allo scopo di limitare l'accesso ai soli soggetti strettamente autorizzati; - Conservazione dei dati per un periodo strettamente limitato al loro utilizzo, a conclusione del quale dovranno essere rimossi e se oggetto di modifiche dovranno essere allineati con i dati originali; - annotazione di tutti i supporti informatici mobili che vengono utilizzati con l'indicazione del soggetto responsabile a cui viene affidato e delle finalità di utilizzo.

18. COMUNICAZIONE E TRASMISSIONE DATI MEDIANTE APPLICAZIONI DI MESSAGGISTICA ISTANTANEA (WhatsApp, messenger, telegram, Instagram, ecc)

Utilizzo di messaggi contenenti dati e informazioni personali

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
Scambio di informazioni mediante l'utilizzo di applicazioni che consentono la trasmissione di messaggi istantanei a singoli destinatari o a gruppi. Tali comunicazioni, ancorché effettuate con dispositivi forniti dall'amministrazione, se utilizzano applicazioni che non forniscono le necessarie garanzie di sicurezza e riservatezza non possono contenere informazioni di carattere personale, né di carattere riservato. Dovrà essere riconosciuta particolare attenzione anche nel caso di trasmissione di documenti o qualsiasi altra informazione in quanto i sistemi comunemente utilizzati non assicurano alcuna riservatezza e consentono al gestore particolare autonomia nell'utilizzo e nella destinazione dei dati trattati.	L'utilizzo di applicazioni di messaggistica istantanea si configura inevitabilmente come la trasmissione di dati e informazioni a un soggetto esterno che non risulta in alcun modo autorizzato al trattamento, né è chiamato a rispondere sulle modalità di utilizzo delle informazioni che riceve.	- eventuale indebita divulgazione, sia volontaria che involontaria, delle informazioni a soggetti esterni; - perdita di disponibilità dell'informazione con il rischio di permanenza illimitata presso dispositivi esterni	1) utilizzo, se disponibili, di sistemi di messaggistica protetti che forniscano garanzie di riservatezza 2) limitazione delle informazioni oggetto dei messaggi a quelle strettamente necessarie e in ogni caso che non riguardino dati personali o documenti oggetto di segreto di ufficio

19. TRASMISSIONE E NOTIFICA DI ATTI A PERSONA DIVERSA DAL DESTINATARIO

Consegna di un documento ai fini della ricezione formale o notifica a un soggetto diverso rispetto al destinatario

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
La comunicazione, trasmissione o notifica di atti a soggetti diversi dai destinatari deve essere effettuata, sia nel rispetto delle prescrizioni normative, generali o specifiche, relative alla registrazione della consegna e avvenuta notifica, sia nel rispetto del trattamento dei dati personali. E' richiesta attenzione agli atti che contengono dati personali da cui si possano evincere sanzioni per specifici comportamenti, stati di salute, condizioni fisiche, disagio economico sociale, valutazioni sul comportamento o sull'esito di prove selettive o qualsiasi altra informazione di carattere personale. Per gli atti di cui sopra l'attività di comunicazione e/o notifica dovrà essere effettuata avendo cura di consegnare l'atto direttamente al destinatario. Qualora ciò non sia possibile, la consegna dovrà essere effettuata solo a persona autorizzata a riceverlo, nel rispetto della normativa vigente, avendo cura di consegnare la documentazione in busta chiusa	Se la consegna o la notifica avviene mediante il ricorso a soggetti esterni all'ente, a cui è affidata tale operazione (per esempio: postalizzazione, notifica, ecc.) è necessario che ciò sia "rigorosamente" disciplinato da un atto formale in cui si definiscono sia l'oggetto dell'affidamento, sia le modalità di attuazione, sia le rispettive responsabilità riguardo al trattamento dei dati personali. Inoltre, l'interessato dovrà essere messo al corrente (mediante la predisposizione e diffusione di un'informativa) riguardo al trattamento dei propri dati affidati a un soggetto estraneo ai fini della notifica.	- eventuale consegna a soggetto errato o non autorizzato - eventuale visione del documento, totale o parziale, da parte di un soggetto diverso dall'interessato - eventuale indebita divulgazione dei dati personali - eventuale smarrimento del documento da trasmettere o notificare	- predisposizione di plichi sigillati che non consentano l'accesso al contenuto - registrazione dell'avvenuta consegna e delle generalità del soggetto a cui viene consegnato - disciplinare contenente le prescrizioni da adottare, nel caso di affidamento della consegna o notifica a un soggetto esterno - predisposizione di una informativa che contenga le indicazioni del soggetto esterno a cui è affidata l'operazione di notifica

20. GESTIONE CORRISPONDENZA ANALOGICA (NON DIGITALE) RISERVATA

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
il trattamento ricorre nel caso in cui a qualsiasi ufficio dell'ente perviene una busta cartacea con l'indicazione "riservata". Tale dicitura rivela inequivocabilmente l'intenzione del mittente di indirizzare a una persona specifica un messaggio il cui contenuto si richiede che non venga divulgato. Conseguentemente per tale forma di corrispondenza deve essere prescritta una procedura che assicuri la corretta destinazione del plico nel rispetto delle esigenze di riservatezza. Resta inteso che il destinatario della missiva, una volta avuta cognizione della corrispondenza, se correttamente acquisita, sarà responsabile della divulgazione totale o parziale del contenuto. A tal fine si riporta di seguito integralmente la prescrizione contenuta nell'art. 616 del Codice Penale "Chiunque prende cognizione del contenuto di una corrispondenza	I soggetti esterni all'ente, così come gli impiegati dello stesso ente, se coinvolti nella trasmissione della corrispondenza, sono tenuti ad assicurare sia l'integrità del plico, sia la corretta destinazione.	- apertura, sia volontaria che involontaria, del plico - errata destinazione del plico - smarrimento del plico	- divieto di apertura o manomissione del plico da parte di un soggetto diverso dal destinatario - conservazione del plico in condizioni di integrità fino alla consegna al corretto destinatario

21. GESTIONE CORRISPONDENZA DIGITALE

modalità di trattamento	ricorso a soggetti esterni	rischi probabili	misure di prevenzione
Il trattamento riguarda la ricezione volontaria o involontaria di una corrispondenza privata pervenuta per errore o comunque rivolta ad un destinatario diverso. Anche se in forma telematica la corrispondenza personale e riservata deve essere trattata avendo cura che sia correttamente indirizzata e che la visione sia effettuata esclusivamente dal destinatario. Nel caso in cui un soggetto, sia intenzionalmente, sia involontariamente, ha cognizione di una comunicazione digitale rivolta ad altre persone è tenuto a informare di ciò il destinatario avendo cura di trasmetterne il contenuto e di rimuoverla dai propri archivi. A tal fine si riporta di seguito integralmente la prescrizione contenuta nell'art. 616 del Codice Penale "Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae. al fine di	I soggetti esterni all'ente, così come gli impiegati dello stesso ente, Sono tenuti ad assicurare che la corrispondenza erroneamente pervenuta sia inoltrata al soggetto destinatario con l'impegno di rimuoverla una volta accertata l'effettiva destinazione	- acquisizione, cognizione, conservazione e divulgazione di un messaggio rivolto ad un soggetto diverso - perdita di una comunicazione inoltrata a un destinatario diverso	- divieto di acquisizione, cognizione, conservazione e divulgazione di messaggi digitali rivolti a destinatari diversi - nel caso di corrispondenza erroneamente inoltrata, obbligo di indirizzarla al destinatario corretto