PROVINCIA
DI REGGIO EMILIA

MANUALE MINIMO

DEL TRATTAMENTO

DEI DATI PERSONALI

Il nuovo Regolamento generale per la protezione dei dati personali 2016/679 (UE), noto dall'acronimo inglese, come GDPR (e così lo chiameremo d'ora in poi), sta imprimendo una svolta importante nella cultura e nelle pratiche della protezione dei dati personali.

Dalla precedente direttiva europea del 1995 nella stessa materia il mondo dell'informazione è cambiato più volte: si sono diffusi prima internet, le reti dati e gli strumenti di posta elettronica, poi i social, il commercio elettronico e l'economia digitale.

Principi e obiettivi della protezione dei dati non sono cambiate, ma le minacce, i rischi e le sfide sono diventati molto più impegnative.

Anche la cultura della pubblica amministrazione sta cambiando: chi lavora al suo interno vive il cambiamento dell'informazione e, inevitabilmente, porta dentro gli uffici una sensibilità più accentuata e una maggior consapevolezza dei problemi e delle criticità.

Questo Manuale minimo riprende precedenti documenti della Provincia di Reggio Emilia adeguandone i contenuti al nuovo regolamento.

Nella prima parte vengono riassunte le principali novità e continuità del GDPR; nella seconda vengono riprese e aggiornate le indicazioni operative e le istruzioni per un corretto trattamento dei dati.

IL GDPR IN PILLOLE

LE NOZIONI DI BASE DEL REGOLAMENTO GENERALE PER LA PROTEZIONE DEI DATI PERSONALI

SFIDE E RISCHI DELLA SOCIETA' DELL'INFORMAZIONE

La sfida del GDPR è soprattutto quella di far fronte all'evoluzione tecnologica della società dell'informazione, un modo in cui i dati non sono semplicemente uno strumento di lavoro come è sempre stato, ma la più importante risorsa economica disponibile sul pianeta, una vera miniera, che deve essere "scavata" con molte cautele per evitare gravi danni alla dignità delle persone, oltre che alla loro condizione economica.

1. Il nuovo regolamento europeo.

Il nuovo Regolamento generale per la protezione dei dati personali 2016/679 (UE), noto dall'acronimo inglese, come GDPR, ha sostituito dal 25 maggio 2018 il d.lgs. 16/2003 che a sua volta aveva abrogato la l. 675/1996.

Il GDPR non scardina principi e strumenti della disciplina precedente, ma introduce alcune novità che rendono più stringente l'attenzione che occorre portare a questa materia.

LE LEPRINCIPALI NOVITA' DEL GDPR – 1

1. Il principio di responsabilizzazione (accountability): l'idea più innovativa e più rivoluzionaria del GDPR è che i titolari del trattamento (la Provincia nel nostro caso) non posso limitarsi a individuare e adempiere degli adempimenti, ma debbono essere attivi e sempre in grado di dimostrare di aver adottato adeguate misure di tutela dei dati;

2. I titolari di una certa dimensione (tra essi la Provincia) debbono predisporre il Registro dei trattamenti, uno strumento essenziale per tener sotto controllo i flussi dei dati tratti e,, soprattutto, individuare rischi e relative contromisure;

I titolari che avevano adottato corrette strategie e strumenti di trattamento dei dati personali non si troveranno in particolare difficoltà nell'applicazione del GDPR. Nello stesso modo responsabili e incaricati che non si siano limitati al semplice adempimento, ma abbiano curato la cultura del trattamento, non avranno problemi, anche se sarà necessaria un po' di manutenzione straordinaria.

2. I principi del trattamento

Per gli enti pubblici la sfida portata dal GDPR è quella di passare da una visione limitata alla garanzia di un corretto procedimento amministrativo (che comunque è imprescindibile) ad una in cui si comprende che il corretto trattamento dei dati è una componente ormai essenziale della qualità dei servizi resi ai cittadini, soprattutto tenendo conto del contesto della società dell'informazione al quale ci si riferiva prima.

Per questo non basta dotarsi di regole puntuali su come trattare ogni tipo di dato, regole che spesso sono comunque molto utili, ma occorre:

a) fare propri i principi del trattamento in modo che saltino agli occhi i comportamenti scorretti o semplicemente superficiali e ciascuno sia capace di adottare le necessarie contromisure;

b) integrare nella prassi amministrativa i principi del trattamento dati per poterne tener conto nel disegno e organizzazione dei procedimenti.

Semplificando il trattamento deve essere **lecito** (avere una base legale che consenta di trattare quei dati, contratto, consenso, norma di legge, ecc.), avere una specifica **finalità** che non può essere sviata (non posso utilizzare un dato rilasciato per uno scopo, per svolgere altra attività), garantire i **diritti** degli interessati e limitarsi ai dati strettamente **necessari** e **pertinenti** alla finalità da raggiungere.

I PRINCIPI

Il GDPR stabilisce che i dati debbano essere:

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; («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); esatti e, se necessario, aggiornati («esattezza»);

d) 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 («limitazione della conservazione»);

e) 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»).

3. I dati personali

Si considera **dato personale** qualsiasi informazione riguardante una persona fisica identificata o identificabile, direttamente o indirettamente: lo spettro è evidentemente molto ampio. Facendo riferimento a persone "identificabili", qualunque elemento riconducibile ad una persona, al momento ancora ignota, va protetto: una foto anonima è un dato personale soggetto a protezione.

Da questi dati personali, considerati ordinari, vanno distinte le **particolari categorie di dati** che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona ; sono quelli che la precedente disciplina definiva dati sensibili. Non cambia l'esigenza di una particolare tutela di questi dati.

Vanno infine distinti i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza; si tratta dei vecchi "**dati giudiziari**"; anche in questo caso si richiudono tutele particolari.

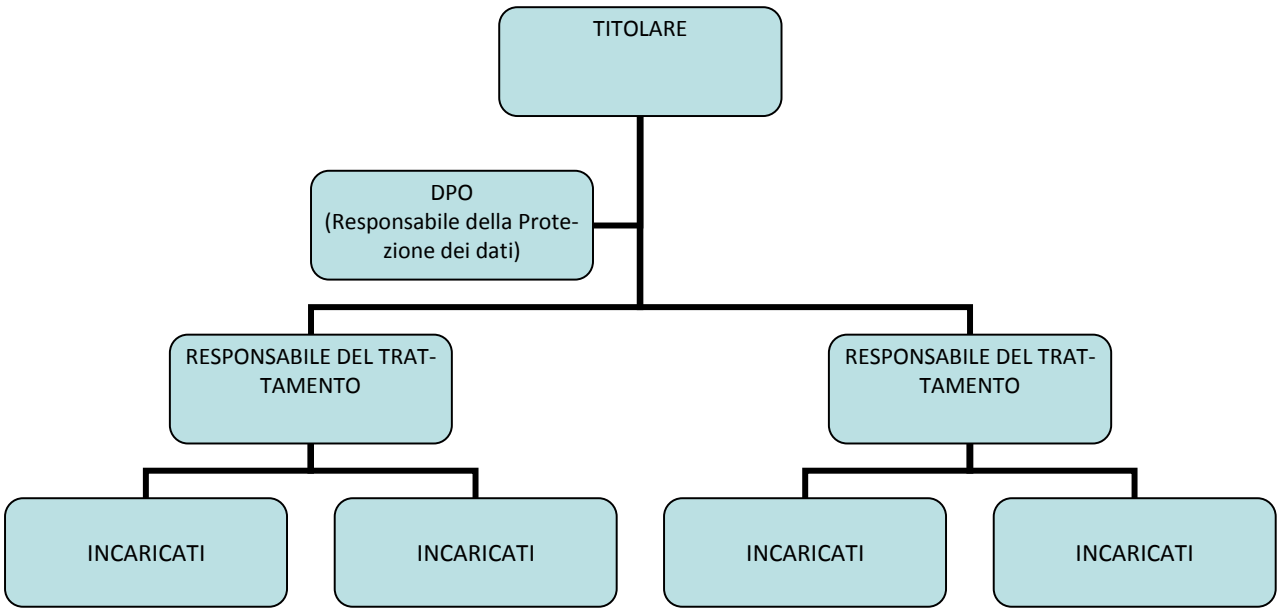
4. L'informativa

Gli enti pubblici non necessitano del consenso degli interessati per trattare i loro dati purché il trattamento sia richiesto per l'esecuzione di un compito di pubblico interesse, per i dati ordinari, o sia necessario per motivi di interesse pubblico. In ogni caso occorre rilasciare agli interessati l'**informativa** con la quale essi sono messi a conoscenza:

a) dell'identità del titolare del trattamento;
b) delle finalità perseguite dal trattamento;
c) dei soggetti ai quali i dati potrebbero essere trasferiti.

5. L'organizzazione

Il GDPR, come già prima il d.lgs. 196/2003, prevede che ogni ente o impresa che tratta dati di terzi (gli "interessati") si dia una precisa organizzazione a tutela del corretto trattamento.
Al vertice si colloca il **titolare del trattamento**, nel nostro caso la Provincia di Reggio Emilia, che nelle sue varie articolazioni (consiglio, presidente, dirigenti) assume le decisioni strategiche in ambito di trattamento dati: definisce le finalità, garantisce l'adeguatezza degli strumenti di protezione, nomina il DPO e i responsabile del trattamento. I **responsabili del trattamento** sono coloro che sulla base delle indicazioni del titolare organizzano il trattamento assicurando la rispondenza alle scelte del titolare e alla disciplina di legge. I responsabili, infine, autorizzano i propri collaboratori (che nel decreto 196/2003 venivano definiti "**incaricati**") al trattamento dati e assicurano la qualità del loro lavoro. In tutto ciò titolare e responsabili sono assistiti dal **DPO** che orienta l'organizzazione al rispetto dei diritti degli interessati alla riduzione dei rischi.



6. Cosa si intende per trattamento

La nozione di trattamento utilizzata dal GDPR è molto ampia e comprende "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". Questo significa

che l'organizzazione deve essere conoscere il **ciclo di vita** dell'informazione al proprio interno e **tutelarla** adeguatamente durante tutto il percorso: nessuna delle attività elencate è completamente priva di criticità.

In particolare, un ente pubblico deve fare particolare attenzione alle seguenti attività, indipendentemente che il trattamento avvenga con sistemi informatici o analogici (cartacei):

a) la "raccolta di dati", riguarda l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi;

b) il trattamento interno dei dati: raggruppa le varie operazioni poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili. Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- la organizzazione dei dati in senso stretto, cioè il processo di trattamento che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione,….;
- la elaborazione, cioè le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;
- la selezione, la estrazione ed il raffronto, che sono operazioni specifiche che rientrano nella ipotesi più generale della elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni di dati;
- la interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la conservazione dei dati (alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza);
- la cancellazione o la distruzione dei dati, che sono operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni specifici adempimenti;
- gestione delle relazioni con l'interessato.

c) La gestione dei dati verso l'esterno:

- la comunicazione a terzi, cioè portare a conoscenza i dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione;
- la diffusione, cioè rendere noti i dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

LEPRINCIPALI NOVITA' DEL GDPR – 2

3. Per dare sostanza al principio di responsabilizzazione, i titolari debbono poi nominare il Responsabile della protezione dati, più noto, sempre per effetto dell'acronimo inglese, con DPO (Data protection officer): si tratta di un consulente dotato di autonomia e adeguata professionalità che indirizzi il titolare nelle scelte di trattamento, garantendo l'aggiornamento normativo e tecnico

4. I processi che trattano dati debbono essere pensati e progettati fin dall'inizio in modo da utilizzare il minimo necessario dei dati e garantirne il corretto trattamento in modo automatico (protezione *by design* e *by default*).

7. Il registro dei trattamenti

Il registro dei trattamenti è una delle novità messe in campo dal GDPR e costituisce uno degli strumenti essenziali dell'accountability, la responsabilizzazione su cui la norma fa perno.

Il registro dei trattamenti è frutto del censimento che ogni organizzazione deve fare delle proprie procedure e quindi di tutti i trattamenti necessari alla propria attività; la rilevanza del registro sta nel fatto che esso deve contenere due informazioni cruciali: da un lato deve indicare i rischi connessi a quei trattamenti e el contromisure adottate dall'organizzazione.

8. I rischi principali

Tutto il sistema di gestione dei dati è costruito per azzerare o, perlomeno, ridurre i rischi che derivano dai trattamenti. Un breve elenco può essere utile per comprendere la complessiva dell'area in cui ci si muove.

Tra i principali rischi possono essere considerati i seguenti:

a) utilizzo di dati legittimamente raccolti per altre finalità (ad esempio, utilizzo a fini commerciali di informazioni raccolte a solo scopo di sottoscrizione contrattuale): è il vero fondamentale rischio nella società dell'informazione, cui gli enti pubblici sono meno esposti, se non per errore o superficialità;

b) raccolta di informazioni eccedenti il fine: può succedere anche per eccesso di zelo di chiedere più dati del necessario;

c) comunicazione interna a personale non autorizzato, non abilitato o semplicemente non coinvolto nella procedura;

d) accesso dall'esterno ai dati con relativa sottrazione;

e) perdita o distruzione volontaria (dolo) o involontaria (colpa) di informazioni;

f) comunicazione a terzi non autorizzata o non necessaria a fini istituzione;

g) diffusione non autorizzata o non necessaria a fini istituzione; questo rischio e il precedente sono particolarmente rilevanti e gravi in caso di dati particolari (sensibili) o giudiziari.

ISTRUZIONI E REGOLE DI COMPORTAMENTO PER IL TRATTAMENTO DEI DATI

Le istruzioni e le regole che seguono, alle quali il personale della Provincia deve attenersi, costituiscono il primo e fondamentale strumento di riduzione del rischio.

E' importante seguire queste istruzioni, ma lo è ancor più farlo tenendo conto che quando trattiamo dati personali abbiamo sempre a che fare con la dignità delle persone e, talvolta, anche con il loro portafoglio.

L'accesso ai dati personali, compresi i dati particolari (per comodità continueremo a chiamarli "sensibili" anche se questa espressione non è presente nel GDPR) e giudiziari è autorizzato nei limiti in cui le operazioni e le informazioni siano necessarie per il corretto svolgimento delle attività affidate, nonché per l'esecuzione dei compiti istituzionali del servizio di appartenenza.

1. Le Regole di comportamento e le istruzioni per lo svolgimento delle operazioni di trattamento riguardano:

1. **l' obbligo del segreto**: la regola fondamentale per garantire la tutela della riservatezza e della vita privata di persone fisiche e giuridiche è il segreto. Pertanto, ciascun dato o informazione, oggetto di conoscenza o di acquisizione, anche indiretta (come ad esempio nei casi di colloqui, visione di documenti, movimentazione di fascicoli, consegna a mano di corrispondenza,…), non deve essere utilizzato, se non esclusivamente per le finalità istituzionali e per lo svolgimento di mansioni e compiti relativi al servizio di appartenenza ovvero necessari per l'esecuzione degli obblighi e adempimenti oggetto di contratto di prestazione di servizio;

2. **la raccolta dei dati:** prima di procedere alla raccolta dei dati personali, deve essere fornita **l'informativa all'interessato** o alla persona presso cui si raccolgono i dati, ai sensi dell'art. 13 del Regolamento generale per la protezione dei dati personali 2016/679 (UE) (di seguito GDPR). La Provincia di Reggio Emilia ha predisposto la modulistica da utilizzare pubblicata sulla Intranet dell'Ente e riportata al termine del presente documento con la denominazione *"Informativa per il trattamento dei dati personali"*.

3. **le modalità di raccolta:** occorre procedere alla raccolta dei dati con la massima cura, verificandone l'esattezza, nonché la pertinenza, la completezza e la non eccedenza rispetto alle finalità del trattamento,secondo quanto previsto dalla legge o dai regolamenti e le istruzioni del responsabile di servizio. E' indispensabile non lasciare c.d., d.v.d, chiavette USB o altri supporti informatici, fogli, cartelle o altri supporti di memorizzazione a disposizione di estranei;

4. **le modalità di conservazione**: i documenti o gli atti, che contengono dati sensibili o giudiziari o comunque riservati, devono essere custoditi e conservati in archivi ad accesso controllato. A tal proposito, ciascun responsabile del trattamento deve prevedere misure, da far rispettare ai propri

incaricati, idonee a garantire che armadi, schedari e contenitori siano muniti di serratura ovvero che siano protetti contro accessi non controllati, adottando soluzioni (organizzative e procedurali), che consentano ai soli soggetti incaricati del trattamento di conoscere le informazioni contenute;

5. **le modalità di utilizzo dei dati:** i dati possono essere utilizzati solo dai soggetti espressamente incaricati. L'utilizzo dei dati deve avvenire per scopi determinati, espressi e legittimi e si deve evitare un utilizzo diverso rispetto alle finalità istituzionali dell'ente o non compatibile con le stesse;

6. **le modalità di comunicazione**: con tale espressione si intende "il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". Ciò che caratterizza l'operazione di comunicazione è il fatto che un soggetto determinato (in posizione di terzietà rispetto alla Provincia ed all'interessato) possa in qualunque forma conoscere dati personali riferiti all'interessato medesimo;

7. **la comunicazione di dati sensibili:** i dati sensibili possono essere comunicati a soggetti determinati solo ove sia espressamente previsto da una legge, che autorizzi tale operazione, ovvero dal regolamento sui dati sensibili e giudiziari. In ottemperanza agli artt. 20 e 21 del previgente Codice il Consiglio provinciale ha adottato con deliberazione n. 4/2006 il Regolamento per il trattamento dei dati sensibili e giudiziari ai sensi del D.Lgs. 196/2003, disponibile e visionabile sul sito istituzionale della Provincia di Reggio Emilia; tale regolamento continua a rimanere in vigore per quanto compatibile con il GDPR;

8. **la comunicazione di dati comuni:** la comunicazione di dati comuni (ossia diversi da quelli sensibili) può avvenire solo se espressamente prevista da una legge o da un regolamento. Solamente nei confronti di altri soggetti pubblici, in via residuale, la comunicazione dei dati comuni può avvenire ove sia necessaria per l'esercizio di una finalità istituzionale dell'ente destinatario della comunicazione stessa.

9. **la diffusione dei dati**: con tale espressione si intende " dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione". La pubblicazione di qualsiasi atto (all'albo pretorio o in una bacheca, ovvero in Internet), che contenga dati personali, costituisce una forma di diffusione di informazioni personali ed è possibile solo se prevista da una norma in esecuzione di un compito pubblico. E' comunque vietata la diffusione di dati personali idonei a rivelare lo stato di salute.

10. **esercizio del diritto di accesso**: in caso di richiesta di diritto di accesso ai sensi della l. 241/1990 o del d.lgs. 33/2013, si applica la contemperazione dei diritti sulla base degli art. 59 e 60 del d.lgs. 196/2003.

Qualora un incaricato del trattamento, nello svolgimento della propria attività lavorativa, si trovasse nella situazione di dover procedere ad una comunicazione o alla diffusione di dati, in mancanza di una espressa disposizione di legge o di regolamento o vi siano dubbi al riguardo, sulla co-

pertura normativa, deve rivolgersi al dirigente di servizio, responsabile del trattamento dei dati.

2. Le regole e le Istruzioni per il corretto utilizzo degli strumenti elettronici concernono:

1. **le modalità di utilizzo dei personal computer:** tutte le volte che si abbandona la propria postazione di lavoro, si devono adottare accorgimenti per garantire che i dati trattati e memorizzati con elaboratori informatici non siano accessibili a soggetti non autorizzati. A tal proposito, si ricorda di non comunicare a terzi la propria password di accesso e di adottare misure di protezione: queste possono consistere in uno *screen saver* con password; ovvero nella sospensione della sessione di lavoro, attraverso la disconnessione dell'applicazione in uso;
2. **l'uso della posta elettronica e di internet:** la posta elettronica deve essere utilizzata per scopi istituzionali di ufficio. Si ricorda che qualunque comunicazione ricevuta o spedita utilizzando l'indirizzo di posta della Provincia non ha natura di corrispondenza personale.

In calce ai messaggi di posta elettronica, è opportuno inserire la seguente formula:

AVVISO DI PROTEZIONE

La presente comunicazione può avere natura riservata, per cui i destinatari devono evitare di inoltrare a terzi il messaggio ricevuto, se non previa autorizzazione del mittente o quando vi sia una necessità personale o una giusta causa. Qualora sia stato inoltrato per errore un messaggio ad un soggetto non legittimato, quest'ultimo è pregato cortesemente di darne avviso al mittente e di procedere alla immediata cancellazione del testo dalla propria casella di posta elettronica. Si ricorda che la memorizzazione o la conservazione di informazioni ricevute erroneamente o senza averne titolo costituisce un comportamento sanzionabile dal Regolamento 2016/679 (UE).

3. **la protezione dei dati particolari**: occorre fare particolare attenzione alla spedizione, a mezzo di posta elettronica, di file o di messaggi contenenti dati sensibili. In tal caso, occorrerà proteggere il contenuto del file dall'accesso e dalla visione di soggetti non autorizzati o legittimati al trattamento, diversi dai destinatari delle comunicazioni elettroniche considerate. A titolo meramente esemplificativo, si consiglia (a seconda dei casi, da valutarsi a cura del responsabile del trattamento) il ricorso all'uso di codici identificativi dell'identità dell'interessato associati ai dati sensibili e giudiziari;

4. **i file di log:** per ragioni di sicurezza ed in ottemperanza con la normativa vigente, l'ente dispone di sistemi di tracciamento delle operazioni svolte sui sistemi informativi della rete provinciale.

5. **le istruzioni per l'utilizzo del fax**:
- digitare correttamente il numero di telefono, cui inviare la comunicazione;
- controllare l'esattezza del numero digitato prima di inviare il documento;
- verificare che non vi siano inceppamenti della carta ovvero che non vengano presi più fogli

contemporaneamente;

- attendere la stampa del rapporto di trasmissione, verificando la corrispondenza tra il numero di pagine da inviare e quelle effettivamente inviate;
- qualora vengano trasmessi dati idonei a rivelare lo stato di salute, può essere opportuno anticipare l'invio del fax chiamando il destinatario della comunicazione al fine di assicurarsi che il ricevimento avverrà nelle mani del medesimo, evitando che soggetti estranei o non autorizzati, possano conoscere il contenuto della documentazione inviata;
- in alcuni casi, può essere opportuno richiedere una telefonata che confermi da parte del destinatario la **circostanza della corretta ricezione e leggibilità del contenuto del fax.** Formula consigliata da inserire in calce alla copertina di accompagnamento delle comunicazioni a mezzo fax:

"Qualora il destinatario del presente fax non sia la persona indicata nella presente copertina, è pregato di dare immediata comunicazione al mittente, a mezzo telefono o per fax. Successivamente, si prega di distruggere la documentazione erroneamente ricevuta, con l'avvertimento che in caso di non ottemperanza a questo invito si potrà essere responsabili della mancanza di protezione o dell'uso non autorizzato delle informazioni erroneamente acquisite".

6. **l'utilizzo del telefono:** è opportuno non fornire dati e informazioni di carattere sanitario o di natura comunque riservata per telefono, qualora non si conosca o non si abbia una verosimiglianza dell'identità o della legittimazione a conoscere del soggetto chiamante. In alcuni casi, può essere opportuno richiedere l'identità del chiamante e la propria qualità, provvedendo a richiamare, al fine di avere la certezza sull'identità del richiedente. Queste precauzioni non valgono nel caso di dati personali soggetti a pubblicazione (si pensi, a titolo meramente esemplificativo, ai dati di graduatorie di concorso, ovvero di selezioni pubbliche – appalti, conferimenti di incarichi), per cui il soggetto chiamante può conoscere i propri dati e quelli riferiti a soggetti terzi senza alcuna limitazione;

7. **l'utilizzo dello scanner o del fotocopiatore multifunzione**: i soggetti che provvedono all'acquisizione in formato digitale della documentazione cartacea (utilizzando ad esempio uno scanner o fotocopiatore multifunzione) devono verificare che l'operazione avvenga correttamente e che il contenuto del documento oggetto di scansione sia correttamente leggibile. Qualora vi siano errori di acquisizione ovvero si verifichino anomalie di processo, occorrerà procedere alla ripetizione delle operazioni. Nel caso in cui il file generato dalla scansione venga salvato su una cartella di rete è indispensabile che venga al più presto eliminato e spostato nelle cartelle di lavoro ad accesso riservato.

8. **i supporti informatici di memorizzazione**, già utilizzati per il trattamento dei dati sensibili e giudiziari, devono essere riutilizzati solo se le informazioni precedentemente contenute non sono più in alcun modo recuperabili, dovendo altrimenti essere distrutti. Tali dispositivi, qualora contengano dati personali, devono essere conservati in contenitori muniti di serratura;

9. **l'uso di software:** è vietato installare e usare qualunque software, anche se scaricato da internet, senza la previa autorizzazione da parte del responsabile del trattamento e del responsabile dell'ente dei sistemi informativi. Si ricorda che l'uso di software contraffatto, ovvero senza

licenza d'uso, costituisce un illecito, sia di natura penale, sia civile, secondo quanto previsto dalla legge sul diritto d'autore.

10. **la spedizione di documenti contenenti dati personali a mezzo posta:** la documentazione contenente dati sensibili o giudiziari deve essere trasferita, anche all'interno dell'ente, in busta chiusa, in modo da proteggere la riservatezza del documento e dei dati contenuti. I lembi della busta devono essere sigillati e firmati per garantire l'integrità del contenuto.

3. Regole per operatori di front-office e per la gestione di documenti cartacei:

Gli operatori di sportello o di front-office sono tenuti ad osservare le seguenti prescrizioni per:

1. **il rispetto della distanza di sicurezza** : deve essere prestata particolare attenzione al rispetto dello spazio di cortesia e se del caso invitare gli utenti a sostarsi dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;

2. **l'identificazione dell'interessato**: nei rapporti di sportello con l'utenza può essere necessario identificare il soggetto interessato al fine di verificare l'identità della persona e garantire l'esattezza del dato da raccogliere. A tal proposito è legittimo richiedere ed ottenere un documento di identità o di riconoscimento;

3. **il controllo dell'esattezza del dato:** occorre prestare attenzione alla digitazione ed all'inserimento dei dati identificativi e personali degli interessati, evitando errori di battitura che potrebbero creare problemi nella gestione dell'anagrafica e nel proseguo del processo;

4. **la tenuta di cartelle e di fascicoli:** nei casi in cui gli operatori ricevono nella propria stanza utenti e cittadini, le cartelle ed i fascicoli devono essere trattati in modo da garantire la riservatezza dei dati contenuti;

5. **distruzione delle copie cartacee**: occorre evitare di gettare la documentazione nel cestino della carta senza aver previamente provveduto a rendere inintelligibile il contenuto. Si potranno utilizzare apparati distruggi-documenti o altri sistemi (ad esempio provvedere a stracciare i documenti; separare il dato identificativo dal resto delle informazioni mediante separazione fisica dei fogli..).

4. Misure di protezione dei dati e degli strumenti elettronici:

Tutti gli operatori sono tenuti al rispetto delle seguenti modalità di protezione dei dati mediante:

1. **password**:
- la password, assegnata a ciascun incaricato, deve essere composta da un minimo di otto caratteri o comunque dal numero massimo di caratteri consentito dal sistema;
- la password deve essere autonomamente cambiata dall'interessato ogni tre mesi;

- la password non deve contenere riferimenti agevolmente riconducibili all'incaricato e dovrebbe essere generata preferibilmente senza un significato compiuto;
- l'incaricato, nello scegliere la propria password, deve preferibilmente utilizzare lettere maiuscole, minuscole e numeri;
- la password deve essere custodita con la massima attenzione e segretezza e non deve essere comunicata a terzi per alcun motivo o ragione;
- l'incaricato è responsabile di ogni utilizzo indebito o non consentito della password di cui sia titolare;
- ove vi sia la necessità di garantire la disponibilità dei dati e dei documenti a persone terze, deve essere richiesta l'abilitazione al responsabile dei sistemi informativi e ogni incaricato deve poter accedere con la propria credenziale di autenticazione;

2. **back-up:** laddove non è previsto un sistema centralizzato di salvataggio dei dati personali o laddove i dati siano memorizzati su dischi locali (eventualità che deve essere utilizzata soltanto per casi particolari e concordata con il responsabile dei sistemi informativi dell'Ente), occorre procedere con cadenza almeno settimanale alla effettuazione di copie di sicurezza dei dati personali oggetto di trattamento. Si devono utilizzare gli apparati messi a disposizione dell'incaricato e questi deve consegnare i supporti contenenti le copie di salvataggio al soggetto nominato e incaricato della conservazione, ovvero riporre le copie in un contenitore al quale possano accedere solamente soggetti autorizzati;

3. conservazione supporti rimovibili: i supporti utilizzati per la memorizzazione di copie di file di documenti di lavoro non devono essere lasciati in luoghi accessibili. Si consiglia di riporre cd-rom, floppy disk, dispositivi di memorizzazione in cassetti muniti di serratura ovvero di custodire gli stessi in modo da garantire un accesso controllato.