Allegato 1 all'atto di Nomina
PROCEDURA PRIVACY PER RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

Indice

Ambito

Il presente documento si inquadra nell'ambito dei principi contenuti nell'art. 32 del Regolamento 2016/679/UE (*infra* detto "**GDPR**"), applicabili all'ASL di Rieti in qualità di Titolare del trattamento.

Si rammenta che, ai sensi del GDPR, le misure di sicurezza devono "*garantire un livello di sicurezza adeguato al rischio*" del trattamento e che, in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva.

Inoltre, pur non potendo sussistere, dopo il 25 maggio 2018, obblighi generalizzati di adozione di misure "*minime*" di sicurezza (ex art. 33 D.Lgs. 196/2003 "**Codice della Privacy**"), si ritiene, in ossequio al principio di *accountability* e allo scopo di assicurare un livello minimo di protezione dei dati personali, che le misure di cui agli artt. 34 e 35 del Codice della Privacy come meglio precisate nel suo allegato B, debbano in ogni caso essere garantite dal Responsabile in riferimento a qualsiasi trattamento di dati personali di cui l'ASL di Rieti sia titolare.

Si rammenta, infine, che, su indicazione dell'Autorità Garante, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1), lettere c) ed e) del GDPR) possono restare in vigore le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili.

Scopo e campo di applicazione

Il presente documento, strutturato in differenti sezioni, ha l'obiettivo di specificare le istruzioni operative a cui si devono attenere i Responsabili Esterni del trattamento dei dati personali dell'ASL di Rieti (*infra* detti "**Responsabile**" o "**Responsabili**") e coloro i quali con questi collaborano ovvero da questi dipendono, in conformità con la normativa vigente in materia di trattamento dei Dati Personali e con la nomina in tal senso ricevuta dall'ASL di Rieti in qualità di titolare del trattamento (*infra* detta "**Titolare**") di cui il presente Allegato costituisce parte integrante e inscindibile.

Si precisa, comunque, che nel rispetto delle norme e delle istruzioni in tal senso fornite dal Titolare, possono essere eseguite dai Responsabili attività in autonomia purché non comportino una diminuzione del livello generale e specifico di sicurezza né la modifica delle finalità dei trattamenti loro affidati.

Il Titolare, tramite verifiche periodiche affidate al proprio Responsabile per la Protezione dei Dati (*infra* detto "**Dpo**") e/o altro soggetto allo scopo individuato, effettuerà i controlli che riterrà opportuni per vigilare sulla puntuale osservanza della normativa vigente, della nomina e delle presenti istruzioni operative.

Documenti di riferimento

Costituiscono riferimento imprescindibile per questo documento:

- Il D.Lgs. 196/2003 e s.m.i. e i suoi allegati
- Il Regolamento 2016/679/UE

- Ogni altra normativa nazionale, anche emanata ai sensi dell'art. 13 della Legge n. 163 del 25 ottobre 2017, e/o dell'Unione Europea rilevante in materia di tutela della riservatezza e dei dati personali
- I provvedimenti generali e particolari, le linee guida e le autorizzazioni emanate dall'Autorità Garante per la protezione dei dati personali e/o dal Gruppo dei Garanti Europei della privacy
- Ogni procedura e/o regolamento interno all'organizzazione del Titolare rilevante per la tutela della riservatezza e la protezione dei dati personali

Definizioni

- Ai fini del presente documento si intendono applicabili, le definizioni riportate all'art. 4 del GDPR cui espressamente si rimanda ricordando, in particolare, che: Per **"Legge Applicabile"** o **"Normativa Privacy",** si intende 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, nonché alla libera circolazione di tali dati (di seguito, per brevità, "***GDPR***") a far data dal 25.05.2018, nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, anche emanata ai sensi dell'art. 13 della Legge n. 163 del 25 ottobre 2017, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali applicabili alla fattispecie oggetto del Contratto;
- per **"Dati Personali"**: si intendono tutte le informazioni direttamente o indirettamente riconducibili ad una persona fisica così come definite ai sensi dell'art. 4 par. 1 del GDPR, che il Responsabile tratta per conto del Titolare allo scopo di fornire i Servizi di cui al Contratto;
- per **"Categorie particolari di dati" c.d. Dati Sensibili:** si intendono i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche**,** o l'appartenenza sindacale, nonché i dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- per **"Dati relativi alla salute"**: si intendono i dati personali attinenti alla salute fisica e menatale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- per "**Interessato**": si intende la persona fisica cui si riferiscono i Dati Personali;
- per **"Servizi"**: si intendono i Servizi resi dal Responsabile oggetto del Contratto nonché il relativo trattamento dei dati personali, così come meglio descritto nel presente Atto di nomina e nei suoi allegati;
- per "**Titolare**": si intende, ai sensi dell'art. 4, par. 7 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- per **"Responsabile del Trattamento"**: si intende, ai sensi dell'art. 4, par. 8 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- per **"Ulteriore Responsabile"**: si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo (fornitore) rispetto alle Parti, a cui il Responsabile

del trattamento, previa autorizzazione del Titolare, abbia, nei modi di cui al par. 4 dell'art. 28 del GDPR, eventualmente affidato parte dei Servizi e che quindi tratta dati personali;

- per **"Persona autorizzata al trattamento"** o **"Incaricato"**: si intendono le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- per **"Amministratore di sistema"** o "ADS": si intende la persona fisica dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
- per **"Misure di Sicurezza"**: si intendono le misure di sicurezza di cui alla Normativa privacy;
- per "**Trattamento**": si intende, ai sensi dell'art. 4, par. 2 del GDPR, 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.

Istruzioni per le credenziali di autenticazione

Lo scopo di questa sezione è di fornire le istruzioni operative riguardanti il processo di autenticazione informatica ai sistemi del Titolare, ove previsto in favore del Responsabile e, in particolare, per l'utilizzo delle credenziali (di seguito indicate come password).

Ove necessario ai fini dell'esecuzione del Contratto, il Responsabile ha l'obbligo di richiedere per sé e/o per i propri Incaricati, l'assegnazione e/o la disattivazione di una o più utenze informatiche personalizzate che consentano l'accesso, con adeguate misure di sicurezza, agli ambiti di trattamento espressamente e specificamente individuati.

È compito del Responsabile rendere edotti i propri Incaricati del fatto che, qualora si verifichi una prolungata assenza o un imprevisto impedimento dell'Incaricato che, per sopraggiunte necessità di operatività e/o di sicurezza del sistema, renda indispensabile e indifferibile intervenire sulle attività di trattamento/profili allo stesso assegnati, il Responsabile del Trattamento, mediante la collaborazione del Dirigente Responsabile UOSD Sistema Informatico del Titolare, ovvero un soggetto terzo allo scopo espressamente autorizzato dal Titolare o dal Responsabile, potrà disattivare la password assegnata all'Incaricato e accedere ai dati. L'Incaricato, al rientro in servizio, verrà avvertito dell'evenienza e sarà tenuto alla sostituzione della password non più attiva.

Il processo di autenticazione descritto in questa sezione prevede l'inserimento di un codice identificativo personalizzato dell'Utente (Persona autorizzata o Incaricato), c.d. "user-id", associato a una parola chiave riservata, c.d. "password".

Password Iniziale

- La prima password viene comunicata dagli ADS in modalità riservata all'Incaricato con comunicazione che invita ad effettuare immediatamente la sostituzione.
- La prima password ha carattere provvisorio; non abilita ad alcuna operazione diversa da quelle strettamente necessarie alla sua sostituzione da parte dell'Incaricato.

- L'Incaricato non può e non deve effettuare alcuna operazione se prima non ha provveduto a sostituire la password iniziale.
- L'incaricato effettua la sostituzione della prima password attenendosi alle raccomandazioni fornite nell'Allegato 1 della presente procedura.

Lunghezza e complessità della password

La lunghezza minima della password deve essere almeno di otto caratteri alfanumerici e deve inglobare almeno una lettera maiuscola, una minuscola, un numero e un carattere speciale (es.: !"£$%&/=?^*§ç). Nel caso in cui il sistema non consenta l'utilizzo di una password di otto caratteri, deve essere utilizzato un numero di caratteri pari al massimo consentito.

Scelta e costruzione della password

La password scelta non deve essere banale o facilmente individuabile o riconducibile all'Interessato (data di nascita, codice fiscale, compleanno dei figli, ecc.) pertanto è necessario attenersi alle raccomandazioni fornite nell'Allegato della presente procedura.

Riservatezza della password

Occorre adottare ogni necessaria cautela per assicurare la segretezza e riservatezza della password. L'Incaricato è tenuto alla custodia delle password attenendosi, in particolare, alle seguenti disposizioni:

- la password è strettamente personale e non può essere comunicata ad altri;
- non è consentita la trascrizione della password su carta o su qualsiasi altro supporto;
- l'Incaricato non deve lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Allontanandosi anche temporaneamente dallo stesso deve provvedere a bloccarlo;
- la perdita, la diffusione o la sospetta compromissione di una password personale deve prontamente essere comunicata al Responsabile S.I. dell'Azienda;

Aggiornamento della password

L'aggiornamento password è consentito esclusivamente all'Incaricato attenendosi alle seguenti disposizioni:

- la password deve essere aggiornata dall'Incaricato al primo utilizzo e successivamente almeno ogni tre mesi;
- dove tecnicamente possibile deve essere concessa all'Incaricato la possibilità di sostituire in qualsiasi momento ed autonomamente le password anche in caso di sospetta compromissione della riservatezza. Ove non tecnicamente possibile, l'Incaricato è tenuto a segnalare immediatamente la necessità al Responsabile S.I. dell'Azienda;
- L' incaricato aggiorna la propria password personale, avvalendosi delle regole fornite nell'Allegato 1, al verificarsi di uno dei seguenti eventi:
    - immediatamente in caso di prima attivazione

- per decorrenza del periodo di validità attribuito alla password (3 mesi)
- su esplicita richiesta del Responsabile S.I. dell'Azienda.

È vietata, senza espressa autorizzazione del Responsabile S.I. dell'Azienda, la sostituzione di una password con una frequenza superiore alle 2 volte al giorno.

Istruzioni per utilizzo Pc

Lo scopo di questa sezione è fornire le istruzioni per la gestione dei Personal Computer.
Non è consentito che due o più Incaricati accedano al sistema informatico, simultaneamente o in maniera differita, utilizzando il medesimo identificativo utente e la medesima password.
Il periodo massimo di non utilizzo della password da parte dell'Incaricato è stabilito in tre mesi.
Al fine di proteggere la sessione di lavoro da utilizzi non autorizzati in sua assenza, l'Incaricato non deve lasciare incustodito e accessibile a terzi lo strumento elettronico. Nel caso in cui, dunque, anche temporaneamente, l'Incaricato debba allontanarsi dalla postazione, dovrà attivare lo screensaver protetto da password, disattivare la propria utenza, o mettere comunque in atto idonei mezzi di protezione che impediscano l'accesso ai dati presenti nel PC. Quando vi sia la necessità di assentarsi in modo prolungato dalla propria postazione di lavoro, oltre che attivare gli idonei mezzi di protezione sopra citati, si consiglia, ove possibile, di chiudere a chiave la porta quando si esce dalla stanza.
Non è consentito archiviare o trattare, neppure temporaneamente, dati personali propri o di terzi non attinenti allo svolgimento dell'attività lavorativa sui sistemi informatici del Titolare o su cui si trattino dati di competenza del Titolare.
L'Azienda non risponderà della perdita di materiale e/o dati strettamente personali, eventualmente archiviati nella propria postazione di lavoro.
Ulteriori disposizioni e/o informazioni in riferimento a quanto precede possono essere contenuti in apposite procedure aziendali che verranno messe a disposizione del Responsabile.

Istruzioni per la gestione dei supporti di memorizzazione rimovibili

Lo scopo di questa sezione è di fornire le istruzioni operative riguardanti la gestione dei supporti di memorizzazione rimovibili: hard disk dei personal Computer, CD ROM, penne USB, ecc.
Prima di procedere al riutilizzo per altri scopi lavorativi e autorizzati dei supporti di memorizzazione e nel caso fosse necessario conservare le informazioni contenute negli stessi, deve essere effettuato il salvataggio dei dati sui sistemi informatici Aziendali.
I supporti di memorizzazione prima di essere riutilizzati, devono essere completamente reinizializzati, di modo che le informazioni precedentemente contenute non siano recuperabili e tecnicamente ricostruibili in alcun modo.
I supporti di memorizzazione utilizzati per il trattamento di dati personali di natura sensibile ovvero per la gestione dei dati relativi al personale del Titolare non possono essere riutilizzati per scopi diversi e, nel caso di definitiva dismissione, adeguatamente distrutti per rendere assolutamente irricostruibili le informazioni negli stessi anche solo temporaneamente custodite.

Gli Incaricati hanno la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk

- segnalare la necessità di un'eventuale dismissione dei supporti USB
- segnalare la necessità di un eventuale riutilizzo degli hard disk, dei CD-ROM e dei supporti USB
- eseguire la reinizializzazione dei supporti USB per poterli successivamente riutilizzare ove consentito
- effettuare il test sulla reinizializzazione dei supporti USB eseguita precedentemente.

Istruzioni per il trattamento dei documenti cartacei

II Responsabile dovrà provvedere a:

- identificare gli eventuali soggetti ammessi ad accedere ai Dati Personali detenuti su supporto cartaceo al di fuori dell'orario di lavoro;
- identificare e comunicare al Titolare gli archivi presso l'unità, dove riporre i documenti contenenti i Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, (armadi, stanze, casseforti, ecc.);
- prevedere la conservazione dei documenti contenenti "categorie particolari di dati personali", c.d. Dati Sensibili, separata dai documenti contenenti Dati Personali comuni;
- verificare, previa consultazione con il Titolare, la corretta esecuzione delle procedure di distruzione dei documenti quando non più necessari o quando richiesto dall'interessato.

II Responsabile del trattamento, cosi come gli stessi Incaricati dovranno inoltre provvedere a:

- trattare i Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Giudiziari secondo il principio di necessità, ovvero unicamente per lo scopo per cui sono stati raccolti;
- non diffondere o comunicare i Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili e/o Giudiziari a soggetti non autorizzati al trattamento;
- non lasciare incustoditi documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili e/o Dati Giudiziari durante e dopo l'orario di lavoro;
- non lasciare in luoghi accessibili al pubblico i documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili e/o Giudiziari;
- riporre i documenti negli archivi quando non più operativamente necessari;
- limitare allo stretto necessario l'effettuazione di copie e/o la trasmissione all'esterno dei suddetti documenti.

La riproduzione di documenti contenenti "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Giudiziari su supporti non informatici (ad esempio fotocopie) è vietata se non assolutamente indispensabile per l'esecuzione del Contratto. La riproduzione deve essere sottoposta alla medesima disciplina dei documenti originali.

Nel seguito sono evidenziate le disposizioni che il Responsabile e gli Incaricati devono applicare e rispettare quando trattano documenti cartacei contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Dati Giudiziari.

Archiviazione dei documenti cartacei

I documenti cartacei devono essere:

- conservati in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato dei documenti cartacei, garantendo, quindi, la riservatezza e l'integrità dei Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Dati Giudiziari, in essi contenuti
- riposti negli appositi archivi che dovranno essere chiusi a chiave, in armadi o stanze, al termine della giornata lavorativa. Le chiavi dovranno essere risposte in un luogo sicuro e non lasciate nelle serrature stesse
- trasferiti presso gli archivi centrali quando non più operativamente necessari.

Consultazione dei documenti cartacei

La consultazione dei documenti contenenti Dati Personali e/o "categorie particolari di dati personali", c.d. Dati Sensibili, e/o Dati Giudiziari, deve avvenire esclusivamente da parte degli Incaricati, solo quando operativamente necessario e quando possibile *in loco*.
L'Incaricato può effettuare la consultazione di tali documenti fuori orario di lavoro solo se preventivamente autorizzato dal Responsabile, identificato e registrato dalla vigilanza.

Distruzione dei documenti cartacei

Tutti i documenti che non devono essere conservati per legge, devono essere distrutti al termine della loro utilizzazione.
La distruzione dei documenti nei limiti consentiti dalia legge, deve essere effettuata quando è espressamente richiesto dall'interessato e/o quando comunicato dal Titolare ovvero dal Responsabile, all'interno della propria area di competenza.
I documenti dovranno essere distrutti, sotto la supervisione del Responsabile all'interno della propria unità.
La distruzione dei documenti cartacei contenenti "categorie particolari di dati personali", c.d. Dati Sensibili e/o Dati Giudiziari deve essere effettuata, attraverso opportuni strumenti (distruggidocumenti), in modo da rendere impossibile la ricostruzione del documento.

Allegato 1 - RACCOMANDAZIONI PER LA CREAZIONE DELLE PASSWORD

1. Le password devono essere costruite utilizzando caratteri alfabetici, numerici e simboli speciali disponibili con le tastiere di utilizzo comune.
2. Le password devono contenere almeno un carattere appartenente a ciascuno degli insiemi sopra enunciati.
3. Nei casi in cui non risulti possibile l'utilizzo dei simboli speciali, le password devono contenere caratteri numerici ed alfabetici ripartibili in numero compreso tra un minimo di 3 ed un massimo di 5, ferma restando la lunghezza minima complessiva fissata in 8 caratteri.
4. Le password non devono contenere più di 3 caratteri uguali consecutivi.
5. Le password non devono contenere caratteri di spaziatura.
6. Le password non devono contenere:
    a. nomi propri di persona;
    b. sigle di funzioni organizzative o progetti interni all'Azienda;
    c. nomi di giorni della settimana, mesi dell'anno o stagioni;
    d. nomi di riferimenti geografici;
    e. nomi di personaggi della politica, sport, cinema e fumetti.
    f. riferimenti alla user-id;
    g. il nome o cognome dell'incaricato;
    h. le matricola dell'incaricato;
    i. la data di nascita dell'incaricato, del coniuge o dei figli;
    j. esclusivamente date in qualsiasi formato e con qualsiasi separatore di uso comune.
7. Ogni nuova password deve differire dalla precedente perlomeno in 4 caratteri.

Allegato 2 - INCARICATO DELLA CUSTODIA DELLE COPIE DELLE CREDENZIALI

Compiti degli incaricati della custodia delle copie delle credenziali

Il Responsabile nomina, se lo ritiene opportuno, uno o più Incaricati della custodia delle copie delle credenziali.
Questi, tra i compiti affidati, devono:

- custodire in luogo chiuso e protetto e in busta chiusa le credenziali per l'accesso ai dati degli Incaricati;
- istruire gli Incaricati sull'uso delle parole e sulle caratteristiche che le password debbono avere e sulle modalità per la loro modifica in autonomia.

Nomina degli incaricati della custodia delle copie delle credenziali

Qualora il Responsabile ritenga di non delegare nessun Incaricato della custodia delle credenziali, ne assumerà direttamente le responsabilità e funzioni.
L'incarico viene affidato con lettera d'incarico, controfirmata per accettazione, e conservata il luogo sicuro a cura del Responsabile.
Il Responsabile consegna a ciascun Incaricato della custodia delle credenziali copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina dell'Incaricato della custodia delle credenziali è a tempo indeterminato e decade per revoca o dimissioni dello stesso.
La nomina dell'Incaricato della custodia delle credenziali può essere revocata in qualsiasi momento dal Responsabile o dal Titolare senza preavviso ed eventualmente affidata ad altro soggetto,