

**Regolamento per la disciplina attuativa del codice della privacy D. Lgs 196/2003 e del D.lgs 10 Agosto 2018 recante “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, regolamento europeo GDPR 679/2016 presso il Comando VF di Latina.**

Si pone in evidenza che sono da tempo sono in vigore le norme indicate nel D.Lgs 30 giugno 2003, n. 193 "Codice in materia di protezione dei dati personali" e del regolamento europeo GDPR 679/2016.

Le normative citate dispongono che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Pertanto nell'osservare che la finalità dei suddetti regolamenti non è quella di impedire il trattamento dei dati personali ma piuttosto quella di garantire che le operazioni di trattamento si svolgano secondo determinate modalità poste a tutela della sfera della riservatezza delle persone, essi dispongono che il trattamento dei dati personali debba dunque essere svolta da soggetti autorizzati, nonché ad evitare che dalla conoscenza delle informazioni in essi contenute possa derivare pregiudizio per l'individuo interessato, al quale la legge fornisce peraltro importanti poteri di controllo, di informazione e di intervento.

**Per dato personale si deve intendere** *"qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".* Il dato personale è in sostanza un'informazione relativa a fatti, stati o qualità riguardanti l'individuo.

Per dato sensibile si intende quel sottoinsieme dei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute o la vita sessuale"

**Per dati giudiziari** si intendono invece *" i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettera da a) a o) e da r) a u), del decreto del Presidente della Repubblica del 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.*

Se ne deduce che siano assimilabili ai dati sensibili, sopra richiamati, i dati giudiziari, cioè quelli idonei a rivelare l'iscrizione nel casellario giudiziale dei seguenti atti:

1. sentenze di condanna e decreti penali appena divenuti irrevocabili;
2. provvedimenti emessi dagli organi giurisdizionali dell'esecuzione, non più soggetti ad impugnazione, riguardanti la pena, le misure di sicurezza, gli effetti penali della condanna, l'applicazione dell'amnistia e la dichiarazione di abitabilità o professionalità nel reato o di tendenza a delinquere
3. provvedimenti riguardanti l'applicazione di pene accessorie

**Il Titolare** dei dati è *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, ovvero colui il quale decide se, con quali finalità, con quale ampiezza e con quali modalità effettuare il trattamento dei dati, determinando i destinatari delle informazioni ed i sistemi di sicurezza"*

**Il Responsabile dei dati** è *"la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposto dal titolare al trattamento dei dati personali"*

Gli **Incaricati** sono *"le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile"*

Incaricato è colui che materialmente opera sui dati personali, limitatamente a quelli afferenti alle sue competenze

**l'Interessato** è la persona fisica, la persona giuridica, l'ente o l'associazione a cui si riferiscono i dati personali.

Per **trattamento dei dati** si intende *"qualunque operazione o complesso di operazioni effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati"*

Data l'ampiezza delle operazioni previste dal legislatore, rientra nel campo di applicazione della trattazione ogni tipo di attività riguardante i dati personali, in tutte le sue fasi.

Con il presente regolamento vengono indicate, per il Comando Provinciale, le figure previste dal codice della privacy e che devono essere formalmente incaricate con apposite nomine.

Il Titolare dei dati detenuti dal Comando è il Ministero dell'Interno - Dipartimento dei Vigili del fuoco che opera attraverso il suo legale rappresentante, ovvero il Comandante VF *pro tempore*

Al fine di continuare ad attuare con continuità l'adempimento degli obblighi previsti dal GDPR e dal codice della Privacy, e definire in via generica l'assetto organizzativo in tema di protezione dei dati, **sono individuati quali responsabili del trattamento dei dati**, ciascuno nell'ambito delle proprie competenze e declaratorie da ordinamento del Comando

- Il Funzionario dei ruoli tecnico operativi con incarico di Vicario del Comandante per i dati relativa a attività tecnico operative di soccorso e relazioni esterne
- Il Funzionario dei ruoli tecnico operativi con incarico di Capo Area PST per gli atti di prevenzione incendi
- Il Funzionario dei ruoli tecnico operativi con incarico di Capo Settore per gli atti di Polizia Giudiziaria ONA e Gruppo sportivo
- Il Funzionario dei ruoli tecnico operativi con incarico di Capo Area Formazione interna ed esterna per gli atti relativi
- Il Funzionario dei ruoli tecnico operativi con incarico di Capo Settore per i dati di Affari Generali, e relazioni sindacali.
- Il Funzionario dei ruoli tecnico operativi con incarico di Capo Area RLS per i dati relativi di servizio ed automezzi, attrezzature e scorte di magazzino

- Il Capo Area dell'area amministrativo contabile per le attività ed i dati detenuti dall'area amministrativo contabile, ed i dati sanitari in stretto raccordo con il medico incaricato ed il medico competente per i dati sanitarie l'RSPP.
- Il Capo Settore informatica per l'applicazione del GDPR e la protezione dei dati di qualsiasi natura detenuti esclusivamente su supporto informatico

Il Vicario del Comandante, o altro funzionario di qualifica non dirigenziale che possa svolgere le proprie funzioni in autonomia e indipendenza, nonché in collaborazione diretta con il vertice dell'organizzazione, potrà essere designato quale **RDP (Responsabile della Protezione dei dati interno)** ai sensi dell'art 37 del GDPR **in diretta collaborazione con i Responsabili delle Aree sopra indicati** tenendo conto della complessità dei trattamenti.

Poiché si può osservare che personale VF incaricato, operatori e funzionari che siano addetti a tali uffici sono tutte figure che per necessità istituzionali sono chiamati a *“trattare”* dati personali, alcune volte anche sensibili e giudiziari, a tali figure ***viene ribadito, in qualità di soggetti incaricati e di conseguenza autorizzati di default al trattamento, che le operazioni di trattamento devono svolgersi nel rispetto delle disposizioni contenute nel codice della privacy.***

Si citano alcuni esempi di incaricati alla trattazione di default:

1. addetto amministrativo che effettua il protocollo.
2. funzionario amministrativo che esamina i fascicoli personali del personale permanente o del personale volontario.
3. funzionario tecnico e il funzionario amministrativo che esamina i fascicoli delle procedure per gli acquisti
4. capo partenza che riporta nel rapporto d'intervento VF 41 le generalità di una persona associandola al fatto accaduto.
5. addetto alla sala operativa che registra il nominativo del richiedente l'intervento.
6. funzionario tecnico che esamina una pratica di prevenzione incendi
7. funzionario tecnico o amministrativo che esamina le pratiche previste dal D.Lgs 81/2008
8. funzionario tecnico o amministrativo che esamina le procedure concorsuali.

L'elenco citato non si intende esaustivo.

I dati sensibili e i dati giudiziari che possono essere *trattati* dal Comando sono solo quelli indispensabili per svolgere l'attività istituzionale.

L'interessato ha diritto di ricevere preventivamente una serie di informazioni, la cui elencazione completa è contenuta nell'art. 13 del Codice.

Si evidenzia che per il Comando (Ente pubblico) non è richiesto il consenso all'interessato *solo quando il trattamento dei dati avvenga nell'ambito dello svolgimento delle funzioni istituzionali;*

Inoltre il trattamento deve avvenire entro i limiti posti dalle legge e regolamenti. (Es. Il responsabile o l'addetto di sala operativa che richiede alcuni dati per effettuare l'intervento di soccorso non deve chiedere il consenso per il trattamento dei dati).

Al di fuori delle finalità istituzionali ordinate il trattamento dei dati è in ogni caso non consentito anche in presenza di un eventuale consenso espresso dall'interessato.

In casi di dubbia legittimità si dispone che **il responsabile del trattamento dei dati/Responsabile del procedimento indicato** sopra, predisponga ed invii l'informativa prevista dall'art. 13 del Codice.

Tutte le operazioni di trattamento dei dati devono svolgersi sempre garantendo la riservatezza degli interessati.

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se ancora non registrati e la loro comunicazione in forma intelligibile. L'interessato ha diritto di ottenere alcune indicazioni essenziali: dall'origine dei dati personali, alle finalità e modalità di trattamento, ai soggetti ai quali i dati possono essere comunicati fino all'identità del titolare e del responsabile.

All'interessato vengono riconosciuti ulteriori diritti, in ordine ad esempio alla rettificazione, cancellazione, aggiornamento e trasformazione in forma anonima dei dati. L'interessato può inoltre opporsi per motivi legittimi, in tutto o in parte, al trattamento dei dati che lo riguardano.

Per evitare che i dati personali trattati vengano dispersi e quindi diffusi in maniera incontrollata occorre necessariamente che vengano adeguatamente protetti dai rischi connessi alla loro divulgazione. Pertanto il responsabile e gli addetti devono custodire e controllare i dati personali dai rischi di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità di raccolta.

Con la presente vengono indicate le misure di sicurezza che devono essere attuate immediatamente:

**Per quanto riguarda lo stato di salute ed informazioni del casellario giudiziario**, fra le misure di sicurezza che devono essere predisposte a tutela dei dati che rivelano lo stato di salute dell'interessato o dei suoi familiari (certificati medici ecc), vi è la conservazione discriminata rispetto agli altri dati personali secondo quanto indicato dal codice. Pertanto si dispone, con decorrenza immediata, che nei fascicoli personali del personale permanente e del personale volontario vengano separati, tramite cartelle chiuse, i dati sensibili e giudiziari da quelli personali.

L'accesso ai dati sensibili e giudiziari sia consentito solamente ai soggetti autorizzati dai responsabili alla trattazione degli stessi e solo per le finalità istituzionali.

**Per quanto attiene agli atti afferenti alla liquidazione compensi straordinari, indennità varie, servizi a pagamento ecc**, si può osservare che i dati presenti in tali atti (*indirizzo privato, estremi del conto corrente bancario*) rientrano certamente nella nozione di dato personale.

Pertanto il cedolino contenete i dati delle liquidazioni indicate sopra va consegnato di regola nelle mani dell'interessato o in alternativa vanno adottate opportune tutele della riservatezza che possono consistere, ad esempio, nel piegare e spillare il cedolino, nell'imbustarlo o nel sovrapporvi una copertura delle parti più significati che non riguardano dati di comune conoscenza ( Comando VVF, Sede o ufficio di appartenenza);

Fra le misure di sicurezza che devono essere predisposte a tutela dei dati che rivelano l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale ma anche lo stato di salute, vi è la conservazione discriminata rispetto agli altri dati personali secondo quanto indicato dal codice.

Tra i documenti che riportano dati personali sensibili vi è sicuramente il caso dei certificati medici e dei verbali di visite mediche non prodotti direttamente dagli uffici del Comando ma ricevuti dal Comando in quanto facenti parte di istruttorie di competenza di altri enti, e che devono quindi essere ricevuti per consentirne il solo "trattamento" per gli scopi istituzionali.

Pertanto si dispone, con decorrenza immediata, che questi vengano separati e conservate in cartelle chiuse e di difficile accesso in modo tale che la visione di questi dati sensibili sia consentita solamente al responsabile e agli incaricati del trattamento dell'ufficio.

Nelle graduatorie relative a concorsi o selezioni vanno riportati solamente dati pertinenti (elenchi nominativi abbinati ai risultati, elenchi di ammessi alle prove scritte o orali, non recapiti telefonici e non codice fiscale ecc.). E' sempre vietata la diffusione di informazioni sulla salute del lavoratore o dei suoi familiari. Negli ordini del giorno o altre disposizioni simili devono essere indicati solamente il nome il cognome e il servizio, non recapiti telefonici e non date di nascita.

Nelle Comunicazioni tra il Comando e il lavoratore, per prevenire la conoscenza ingiustificata di dati non autorizzati, i responsabili dei trattamenti dei dati devono adottare forme di comunicazione con il personale protette e individualizzate: inoltrando le note in busta chiusa, inviandole alle e-mail personali o invitando il personale a ritirare personalmente la documentazione.

Per quanto attiene alle Banche dati elettroniche il responsabile ha l'incarico anche della custodia delle parole chiavi e codici identificativi.

Per prevenire la conoscenza ingiustificata di dati non autorizzati nei **fascicoli di prevenzione incendi** deve comparire solamente il numero del fascicoli, inoltre all'interno del fascicoli **devono essere separati i dati della prevenzione incendi da quelli di polizia giudiziaria ( esposti, D.Lgs 758 ecc)**. Si fa presente che gli atti del fascicolo di prevenzione incendi devono essere visionati solamente dal funzionario tecnico; pertanto occorre particolare attenzione nella custodia dei fascicoli all'interno degli uffici dei funzionari tecnici ed è vietato consegnare, da parte del personale dell'ufficio di prevenzione incendi, il fascicolo ai tecnici esterni.

Per prevenire la conoscenza ingiustificata di dati non autorizzati nei fascicoli di polizia giudiziarie e in quelli degli esposti deve comparire solamente il numero del fascicolo. Occorre particolare cura nelle fasi di protocollo, espletamento della procedura ed archiviazione affinché non ci sia diffusione del dato

Per prevenire la conoscenza ingiustificata di dati non autorizzati nello svolgimento delle operazioni di soccorso, occorre particolare cura nelle seguenti fasi:

1. acquisizione dei dati personali o sensibili da parte degli operatori della sala operativa all'atto delle chiamata;
2. compilazione delle relazioni d'intervento;
3. archiviazione delle relazioni d'intervento;
4. trasmissione comunicazioni di intervento.

In queste fasi non deve verificarsi nessuna diffusione di dati personali; in particolare nelle trasmissioni delle comunicazioni di intervento alle varie amministrazioni (Ministero, Direzione Regionale VVF, Prefettura, Comuni ecc) non è necessario, e pertanto non deve essere indicato, nessun dato personale (nome, cognome, data di nascita, proprietario dello stabile, ecc.... ) ma solamente il numero di persone coinvolte, l'indirizzo dello stabile ecc. I dati personali, se necessari, vanno indicati solamente nelle relazione d'intervento VF 41.