*Regione Abruzzo*

# Procedura
# per la Valutazione dei requisiti dei fornitori

della ASL Teramo

in base a quanto previsto dal

## Regolamento UE 2016/679 (GDPR)

| Redazione | Verifica | Parere favorevole | Approvazione |
|---|---|---|---|
| R.T.I. | UOC ABS | D.P.O. | Titolare |

## Sommario

## 1 Introduzione

La normativa vigente in termini di Protezione dei Dati Personali, costituita dal Regolamento UE 2016/679 – Regolamento sulla Protezione dei Dati (di seguito anche il "Regolamento") e dal D. Lgs. 196/2003 – Codice in materia di Protezione dei Dati Personali (di seguito anche il "Codice") come modificato dal D. Lgs. 101/2018, ha l'obiettivo di proteggere i dati personali degli interessati, garantendo che un uso non corretto delle informazioni possa danneggiare o ledere le libertà fondamentali e la dignità degli interessati. Considerato il contesto operativo della ASL 4 Teramo, di seguito denominata "ASL o Azienda Sanitaria", tali problematiche sono di notevole rilevanza.

Le tipologie di dati personali trattati dalla ASL sono costituite principalmente sia da dati personali comuni (esempio dati anagrafici), sia da "particolari categorie di dati personali" (dati sanitari degli interessati).

La ASL predispone il presente documento, nell'ambito del proprio sistema organizzativo a tutela dei dati personali, al fine di soddisfare il principio del privacy by design - Art. 25 del GDPR - (e anche quello del security by design), valutare il rischio relativo ed identificare le misure da prevedere, in caso si ricorra all'affidamento del servizio ad un soggetto terzo che può implicare anche la raccolta, l'elaborazione, l'utilizzo e la conservazione di dati personali.

Nell'ambito del contratto di fornitura standard, attraverso il quale una committente incarica un fornitore di svolgere una determinata attività, che comporti il trattamento dei dati per conto della stessa, la prima sarà identificata quale titolare del trattamento, mentre il fornitore assumerà il ruolo di responsabile del trattamento dati.

In virtù del disposto dell'art. 28 del GDPR, norma sul Responsabile del trattamento, che richiede contenuti determinati per la nomina di tale figura, le parti dovranno necessariamente far riferimento ad un ulteriore e separato accordo attraverso il quale disciplinare nel dettaglio la designazione (si rinvia alla procedura specifica).

## 2 Scopo

Lo scopo della presente procedura è stabilire le responsabilità, i criteri e le modalità con cui la ASL definisce le attività da eseguire per selezionare e valutare i Fornitori, con particolare riferimento alla verifica dei requisiti di sicurezza nel trattamento dei dati personali degli interessati.

## 3 Definizioni

Le seguenti definizioni sono di utilità per poter completare quanto richiesto nell'allegato alla presente procedura questionario in base all'art. 4 del Regolamento:

**«dato personale»:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

**«trattamento»:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione,

l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

**«profilazione»:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

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

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

**«titolare del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

**«responsabile del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

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

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

**«consenso dell'interessato»:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

**«violazione dei dati personali»:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

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

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

**«dati relativi alla salute»:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

**«banca di dati»:** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

**«evento sulla sicurezza delle informazioni»:** occorrenza identificata di uno stato di un sistema, servizio o della rete che indichi una possibile violazione di una policy sulla sicurezza delle informazioni (Information Security Policy) o il fallimento di controlli, o una situazione precedentemente sconosciuta che può essere rilevante a fini di sicurezza;

**«incidente sulla sicurezza delle informazioni»:** evento singolo o serie di eventi sulla sicurezza delle informazioni indesiderati o imprevisti che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni;

**«documento di gara»:** qualsiasi documento prodotto dalle stazioni appaltanti o al quale le stazioni appaltanti fanno riferimento per descrivere o determinare elementi dell'appalto o della procedura, compresi il bando di gara, l'avviso di pre-informazione, nel caso in cui sia utilizzato come mezzo di indizione di gara, l'avviso periodico indicativo o gli avvisi sull'esistenza di un sistema di qualificazione, le specifiche tecniche, il documento descrittivo, le condizioni contrattuali proposte, i modelli per la presentazione di documenti da parte di candidati e offerenti, le informazioni sugli obblighi generalmente applicabili e gli eventuali documenti complementari;

**«DPO»:** Data Protection Officer o Responsabile della Protezione Dati.

**«UOC»:** Unità Operativa Complessa;

**«UOSD»:** Unità Operativa Semplice Dipartimentale;

**«UO»:** Unità Operativa richiedente il lavoro, servizio o fornitura;

**«UO Competente»:** Unità Operativa competente per ambito di riferimento (es.: tecnologico).

## 4 Normativa di Riferimento

La normativa di riferimento per la protezione dei dati personali, nell'ambito della gestione delle procedure di acquisizione di lavori, servizi e forniture, si compone di vari riferimenti relativi al Regolamento UE 2016/679, tra cui:

- Art. 25 - Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

- Art. 32 - Sicurezza del trattamento
- Art. 35 - Valutazione d'impatto sulla protezione dei dati
- Art. 36 - Consultazione preventiva

Le altre normative di riferimento sono:

- D. Lgs. 196/2003 – Codice in materia di Protezione dei Dati Personali (di seguito anche il "Codice") come modificato dal D. Lgs. 101/2018
- Codice degli appalti, D. Lgs. 50/2016 e ss.mm.ii.

## 5 Responsabilità

La responsabilità della corretta applicazione della presente procedura è demandata alle funzioni aziendali coinvolte nella fase attuativa di propria competenza (UOC ABS/UTE/UO procedenti, RUP, DPO e UOC Sistemi Informativi).

## 6 Descrizione del Processo

Premesso che, durante i processi di acquisizione, i fornitori, in relazione alla natura dei servizi offerti, possano accedere al patrimonio informativo delle pubbliche amministrazioni committenti, introducendo potenziali rischi informatici ed organizzativi, con impatto in particolare su riservatezza, integrità, disponibilità, ed autenticità dei dati, ne segue che i processi di acquisizione condotti senza attenzione agli aspetti di sicurezza possono vanificare o, comunque, rendere meno efficaci, le misure prese dal Titolare per tutelare il proprio patrimonio informativo.

Pertanto nell'ambito del procedimento di acquisizione, qualsiasi esso sia, l'area competente dovrà attuare una serie di azioni descritte negli articoli che seguono.

- <u>Classificazione del fornitore</u>

Ai fini della classificazione del fornitore sono identificati due profili possibili, a fronte dei quali verranno richiesti diversi livelli di approfondimento relativamente ai requisiti in materia di misure di sicurezza da applicare al servizio.

La classificazione da adottare è la seguente:

| **Cod.** | **Tipologia di fornitore** | **Utilizzo Infrastrutture** |
|---|---|---|
| 1 | Fornitore Tipo 1 | Fornitori che erogano servizi presso le strutture della ASL o per conto dell'Azienda e che **non utilizzano infrastrutture proprie** |
| 2 | Fornitore Tipo 2 | Fornitori che erogano servizi presso le strutture della ASL o per conto dell'Azienda e che **utilizzano infrastrutture proprie** |

- Valutazione del fornitore relativamente alle misure di sicurezza

La UOC ABS/UTE/UO procedenti, identificata e descritta l'esigenza di acquisto, definiscono le modalità di acquisizione ritenute più opportune, secondo le procedure in essere per l'acquisizione di lavori, servizi e forniture ed in tale fase, effettuano una verifica del fornitore in materia di sicurezza, ossia una valutazione delle garanzie sufficienti per la messa in atto di misure tecniche ed organizzative adeguate, in maniera che il trattamento effettuato dalle terze parti soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Pertanto, le UOC ABS/UTE/UO procedenti dovranno inserire tra la documentazione di gara o della procedura di affidamento, la check list di valutazione "CVF Check list Valutazione Fornitori GDPR" sulle misure di sicurezza in uso presso la propria azienda, allegata alla presente procedura.

In detta Check list il fornitore dovrà prioritariamente dichiarare se, in relazione alla specifica offerta, utilizzi o non utilizzi infrastrutture proprie.

Solo nel caso di dichiarazione di utilizzo delle infrastrutture proprie, il fornitore dovrà compilare tutti i restanti campi per la necessaria analisi di conformità del servizio, lavoro o fornitura rispetto alla normativa sulla protezione dei dati personali (art. 25 Reg. UE 2016/679 – Protezione dei dati fin dalla progettazione e protezione per dei dati per impostazione predefinita) e, in generale, a quella applicabile in materia di sicurezza delle informazioni.

La documentazione richiesta al fornitore è la seguente:

| **Cod.** | **Tipologia Fornitore** | **Utilizzo Infrastrutture** | **Documentazione richiesta** |
|---|---|---|---|
| 1 | Fornitore Tipo 1 | Fornitori che erogano servizi presso le strutture della ASL o per conto dell'Azienda e che **non utilizzano infrastrutture proprie** | nessuna |
| 2 | Fornitore Tipo 2 | Fornitori che erogano servizi presso le strutture della ASL o per conto dell'Azienda e che **utilizzano infrastrutture proprie** | CKL Valutazione Fornitore GDPR (CVF) |

La verifica della presenza e della completezza della check list viene effettuata da parte del RUP nel corso dell'espletamento della procedura.

La valutazione della rispondenza ai requisiti ed alle misure di sicurezza, come richiesta dal GDPR, descritti nella Check list di valutazione GDPR del fornitore, allegata alla documentazione di gara/procedura è a cura del RUP e viene effettuata, nei confronti dell'operatore economico affidatario/aggiudicatario, ai fini della stipula del contratto, previa acquisizione di parere tecnico da parte dell'UOC Sistemi informativi.

Nel caso di parere non favorevole espresso dalla richiamata UOC Sistemi Informativi, la stessa deve indicare i correttivi a cui il fornitore è chiamato ad adeguarsi.

Tutti i correttivi saranno nuovamente oggetto di verifica da parte della UOC Sistemi informativi, al fine di addivenire al definitivo rilascio di valutazione positiva.

In questa fase il Titolare, per tramite dei suoi referenti, può riservarsi di far apportare misure correttive al fornitore al fine di garantire la tutela dei diritti degli interessati ed il DPO fornirà il supporto per ogni controversia, parere o dubbio dovesse sorgere.

In corso di esecuzione del contratto è onere del fornitore segnalare al Titolare, tempestivamente, eventuali modifiche delle misure già adottate.

- Nomina del fornitore come Responsabile del Trattamento (ex art 28)

Successivamente alla fase di valutazione, ~~vi sarà~~ si potrà procedere con la sottoscrizione del contratto e dell'Accordo sulla Protezione dei Dati, ossia l'Atto di designazione del Responsabile del Trattamento, da far sottoscrivere al fornitore contestualmente alla firma del contratto (per il dettaglio del processo di designazione del RT si rinvia alla procedura specifica).

### Adeguamento delle misure in corso di esecuzione

Il Titolare si riserva di effettuare la verifica del mantenimento dei requisiti di sicurezza attivando la procedura di valutazione anzidetta, a campione e sui trattamenti a più alto rischio.

- Valutazione D'Impatto

Qualora il Titolare, tenuto conto della natura del trattamento che andrà ad effettuare il fornitore, sia tenuto ad effettuare la valutazione di impatto sulla protezione dei dati, ai sensi dell'art. 35 del Regolamento, il fornitore dovrà collaborare e fornire tutte le informazioni necessarie per la suddetta valutazione e dovrà anche collaborare nel caso in cui si debba attuare una eventuale consultazione preventiva al Garante, ai sensi dell'art. 36 del Regolamento stesso.

## 7 Conclusioni

Per tutto quanto non contemplato in questa procedura, si rinvia alla vigente normativa di settore in materia di acquisizione beni e servizi e protezione dei dati personali.

In caso di dubbi, contattare il Responsabile della Protezione dei Dati (RPD), raggiungibile al seguente indirizzo: ASL 4 Teramo, con sede in Circ.ne Ragusa n.1, 64100 Teramo, E-mail: dpo@aslteramo.it, Telefono: 0861.420223.

## 8 Allegati

Alla presente procedura sono allegati i seguenti documenti:

- CVF Check list di valutazione GDPR