# Procedura

# per la gestione della conformità in materia di protezione dei dati personali nelle procedure di acquisizione di lavori, servizi e forniture

della Asl 03 Abruzzo

in base a quanto previsto dal

**Regolamento UE 679/2016 sulla Protezione dei Dati (GDPR) e D. Lgs. 196/03 Codice in Materia di Protezione dei Dati Personali**

| | | |
|---|---|---|
| Redazione | Ufficio Privacy/Protezione dati | Dr Vincenzo De Carlo<br>Dr.ssa Simona Taglieri |
| Verifica | Responsabile protezione Dati Personali (RPD/DPO) | Dott. Giovanni Modesti |
| Approvazione | DIRETTORE GENERALE | Dr. Antonio Caponetti |

# Sommario

# 1 Introduzione

La normativa vigente in termini di Protezione dei Dati Personali, costituita dal Regolamento UE 679/2016 – Regolamento sulla Protezione dei Dati (di seguito anche il "Regolamento" o "GDPR") 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 al fine di evitare che un uso non corretto delle informazioni possa danneggiare o ledere le libertà fondamentali e la dignità degli interessati. Considerato il contesto operativo dell'Azienda Sanitaria Locale n.03 di Pescara (di seguito anche la "ASL"), tali problematiche sono di notevole rilevanza.

Le tipologie di dati personali trattati dalla ASL sono costituiti principalmente sia da dati personali (ad esempio dati anagrafici, recapiti, identificativi di tessera sanitaria, codici fiscali, ecc…) che da "particolari categorie di dati personali" (ad es., i dati relativi alla salute).

La ASL predispone la presente procedura di gestione delle Acquisizioni di lavori, servizi e forniture nell'ambito del proprio sistema organizzativo a tutela dei dati personali degli interessati ed in applicazione dei principi applicabili alla Protezione dei dati indicati dall'art. 5 del GDPR.

# 2 Scopo

Il presente documento descrive le modalità operative adottate dalla ASL n.03 di Pescara, per il rispetto di quanto previsto dagli artt. 25, 32, 35 e 36 del Regolamento riguardanti le modalità della verifica della conformità alla normativa sulla Protezione dei Dati Personali nell'ambito delle procedure di acquisizione di lavori, servizi e forniture.

L'obiettivo del presente documento è di fornire una descrizione generale del processo di gestione delle procedure sopra indicate, comprensive delle relative indicazioni operative, al fine di poter consentire alle competenti strutture del Titolare di poter procedere con le azioni di propria competenza.

# 3 Campo di Applicazione

La presente procedura regolamenta il processo di gestione dell'acquisizione di lavori, servizi e forniture che prevedano il trattamento di dati personali da parte delle UU.OO. della ASL di Pescara (ASL n.03 Abruzzo) o che, pur non prevedendo un esplicito trattamento di dati personali, abbiano comunque un potenziale impatto sulla protezione dei dati.

La procedura inoltre si applica anche ai rinnovi contrattuali, estensioni o altra modalità di gestione delle acquisizioni di forniture, lavori o servizi anche a titolo gratuito; in caso di mancata precedente valutazione della tematica relativa alla protezione dei dati personali (es.: acquisizioni precedenti all'entrata in vigore definitiva del Reg. UE 679/2016 – 25/05/2018), sarà necessaria una verifica completa, come nel caso di una nuova procedura di acquisizione.

Anche in caso di procedure di acquisizione concordate a livello regionale, sia nel caso in cui la ASL di Pescara sia capofila, che in caso diverso, l'Azienda dovrà riservarsi la possibilità di effettuare la propria valutazione di conformità rispetto ai requisiti normativi prima della pubblicazione degli atti di gara.

La procedura si intende applicabile alle varie modalità di acquisizione previste dal D.Lgs. 50/2016 e ss.mm.ii. ed applicabili al contesto della ASL 03 di Pescara.

# 4 Normativa di Riferimento

La normativa di riferimento per la presente procedura può essere sintetizzata nel seguente elenco:

- Regolamento UE 679/2016:
  - 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
- D.Lgs. 50/2016 e ss.mm.ii. – Codice dei contratti pubblici
- D.Lgs. 82/2005 e ss.mm.ii. – Codice dell'Amministrazione Digitale

# 5 Definizioni

Le seguenti definizioni sono di utilità per poter meglio comprendere i termini richiamati nella presente procedura. Esse sono tratte dall'art. 4 del Regolamento (UE) 2016/679 e dal Decreto legislativo 18 aprile 2016, n. 50 *Codice dei contratti pubblici*:

1) **«ABS»**: Unità Operativa Complessa Acquisizione Beni e Servizi;
2) **«Autorità di Controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento;
3) **«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;
4) **«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;
5) **«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, i 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;
6) **«DC»**: Dichiarazione di Conformità
7) **«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 preinformazione, 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.
8) **«DPO - RPD»**: Data Protection Officer o Responsabile della Protezione Dati;
9) **«GDPR»**: Regolamento UE 679/2016 – Regolamento Generale sulla Protezione dei Dati Personali
10) **«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;
11) **«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;
12) **«RTD»**: Responsabile della Transizione al Digitale (ex art. 17 Codice dell'Amministrazione Digitale – D.Lgs. 82/2005)
13) **«SAT»**: Soggetto Autorizzato al Trattamento dei dati personali;
14) **«SATD»**: Soggetto Autorizzato al Trattamento dei dati personali con Delega;

15) **«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;
16) **«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;
17) **«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;
18) **«UO richiedente»**: Unità Operativa richiedente il lavoro, servizio o fornitura;
19) **«UO tecnica competente»**: Unità Operativa competente per ambito tecnico/tecnologico di riferimento (es.: tecnologico);
20) **«UOC»**: Unità Operativa Complessa;
21) **«UOSD»**: Unità Operativa Semplice Dipartimentale;
22) **«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.

# 6 Descrizione del Processo

Come previsto dall'art. 25 del GDPR (*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita* – "Data protection by design and by default"), è necessario fare una valutazione dei vari aspetti riguardanti il trattamento (es.: stato dell'arte, costi di attuazione, la natura, l'ambito di applicazione, il contesto, le finalità del trattamento, i rischi per i diritti e le libertà delle persone fisiche), finalizzata all'identificazione di adeguate misure tecniche e organizzative, nei seguenti due momenti:

- determinazione delle finalità e dei mezzi del trattamento;
- esecuzione del trattamento stesso.

L'obiettivo di tali misure è di attuare in modo efficace i principi di protezione dei dati ed integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e della normativa applicabile in materia e tutelare i diritti degli interessati.

Tali misure inoltre devono garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, tenendo in considerazione la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità.

Di conseguenza, il processo di acquisizione di servizi, lavori o forniture, qualunque sia la procedura di acquisizione (bando di gara, acquisizione diretta, convenzione Consip, ecc….), ai fini della verifica di conformità rispetto alla normativa sulla Protezione dei Dati Personali, può essere suddiviso nelle seguenti fasi:

- Fase 1: Definizione dei requisiti per la Protezione dei Dati Personali ed individuazione delle misure di sicurezza
- Fase 2: Dichiarazione di conformità ai requisiti individuati in fase 1 e relativa verifica
- Fase 3: Validazione operativa della conformità del lavoro, servizio o fornitura.

La presente procedura descrive il caso di riferimento principale in cui le esigenze sono comunicate alla UOC Acquisizione Beni e Servizi; nel caso di procedura di acquisizione gestita in autonomia dalle UO Tecnico/Tecnologiche (UOSD Sistemi Informativi, UOC Ingegneria Clinica e UOC Servizi Tecnici Manutentivi), quanto indicato nella presente procedura in capo alla UOC ABS si intende riferito alla UO che procede a gestire direttamente l'acquisizione.

## 6.1 Fase 1: Definizione dei requisiti per la Protezione dei Dati Personali ed individuazione delle misure di sicurezza

L'esigenza di servizi, lavori o forniture viene generalmente manifestata dal Soggetto Autorizzato al Trattamento con Delega (SATD – in genere il Direttore/Responsabile di una UO); tale esigenza, ove preveda una componente tecnica/tecnologica, verrà manifestata alla UOC Acquisizione Beni e Servizi (ABS) con il supporto della competente UO (es.: UOSD Sistemi Informativi, UOC Ingegneria Clinica, UOC Servizi Tecnici Manutentivi) e la previa valutazione da parte del Responsabile della Transizione al Digitale (RTD) il quale potrà esprimere un parere vincolante. Il RTD potrà esprimere un parere negativo in caso di mancato allineamento dell'esigenza rispetto alle linee guida strategiche aziendali o in caso di mancata conformità rispetto alle normative di riferimento in termini di Amministrazione Digitale (es.: Piano Triennale dell'Agenzia per l'Italia Digitale).

Una volta identificata e descritta l'esigenza, questa deve essere comunicata alla UOC ABS per procedere con la modalità di acquisizione ritenuta più opportuna, secondo le procedure in essere per l'acquisizione di lavori, servizi e forniture (D.Lgs. 50/2016 e ss.mm.ii.).

Prima di procedere in via definitiva con la formalizzazione della modalità prescelta, qualora il lavoro, bene o servizio in fase di acquisizione preveda il trattamento di dati personali, o abbia comunque impatto sulla Protezione dei Dati (es.: accesso a locali in cui viene effettuato il trattamento di dati personali), l'UOC Acquisizione Beni e Servizi dovrà sottoporre il «documento di gara» (es.: capitolato, disciplinare, o altra documentazione equivalente, di seguito denominata "documentazione della procedura") all'attenzione dell'UOC Affari Generali e Legali – Ufficio Privacy/Protezione Dati – per la necessaria analisi di conformità.

Nel caso particolare di acquisizione tramite convenzione CONSIP, la documentazione della procedura di acquisizione, che l'UOC ABS dovrà inviare all'Ufficio Privacy/Protezione Dati Personali, consisterà nella Guida alla Convenzione e relativi allegati, unitamente alla richiesta dell'UO richiedente.

I controlli che devono essere effettuati sulla documentazione della procedura, in base alla complessità del/i trattamento/i previsto/i, sono costituiti da una analisi di conformità del servizio, lavoro o fornitura richiesto rispetto alla normativa sulla Protezione dei Dati Personali (art. 25 Reg. UE 679/2016 – *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.

Successivamente a tale verifica, l'Ufficio Privacy/Protezione Dati deve provvedere ad effettuare una analisi e valutazione dei rischi per i diritti e le libertà degli interessati, ai sensi dell'art. 32 del Regolamento UE 679/2016, da cui scaturiranno gli adempimenti e le misure di sicurezza adeguate al livello di rischio identificato.

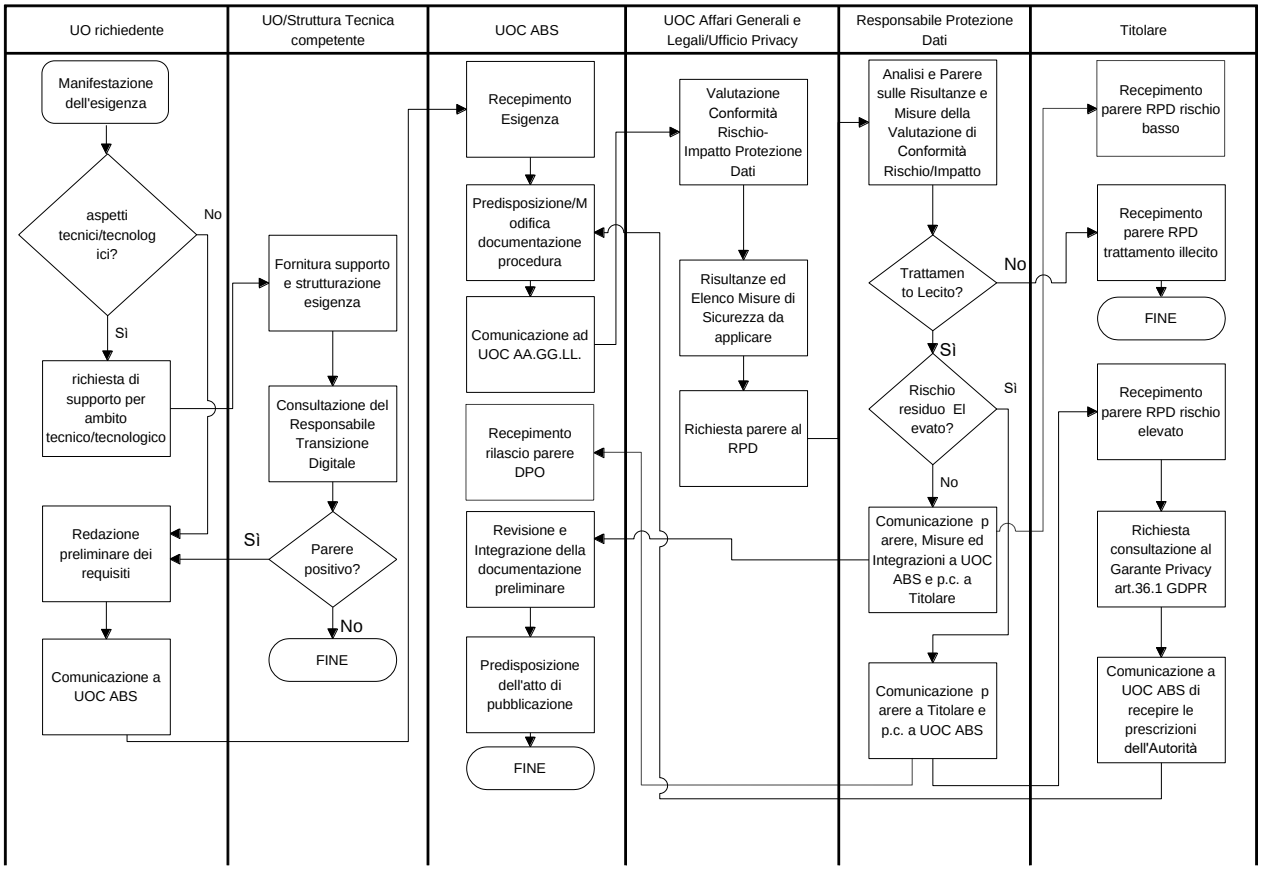
Nei casi previsti dal Provvedimento del Garante n. 467/2018 "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679*", o nel caso in cui il livello di rischio risultante dall'analisi effettuata risulti essere "elevato", all'Ufficio Privacy/Protezione Dati Personali deve effettuare una Valutazione di Impatto sulla Protezione dei Dati ai sensi dell'art. 35 del GDPR.

L'esito di tali valutazioni, inclusivo degli adempimenti e delle misure di sicurezza individuate, in base a quanto previsto dalla normativa, deve essere successivamente sottoposto al parere del Responsabile della Protezione dei Dati aziendale: tale parere potrà essere eventualmente corredato da osservazioni e/o integrazioni; i contenuti della documentazione così prodotta, con particolare riferimento agli adempimenti e alle misure di sicurezza individuate, dovranno essere comunicati al Titolare ed all'UOC ABS e riportati all'interno della documentazione di gara prima della definitiva approvazione e successiva pubblicazione.

All'interno della documentazione di gara, la mancata osservanza degli adempimenti e delle misure richieste in ambito Protezione dei Dati Personali, dovrà essere posta come condizione di risoluzione contrattuale.

Nel caso in cui l'esito delle valutazioni e le osservazioni del RPD non venissero accolte dal Titolare, dovrà essere data opportuna motivazione nell'atto deliberativo di ufficializzazione della procedura di acquisizione.

Nel caso in cui, nonostante le misure individuate, il rischio residuo (per i diritti e le libertà degli interessati) del servizio, lavoro o fornitura oggetto della procedura di acquisizione, risulti essere ancora elevato, il RPD deve comunicare tale eventualità al Titolare per la successiva richiesta di Consultazione all'Autorità Garante per la Protezione dei Dati Personali, ai sensi dell'art. 36.1 del GDPR. L'esito di tale consultazione, secondo la tempistica stabilita dall'art. 36.2 del GDPR, dovrà essere recepito all'interno della documentazione di gara prima della relativa ed eventuale pubblicazione (in caso di indicazione positiva a procedere da parte dell'Autorità Garante per la Protezione dei Dati Personali).




Nell'ambito del flusso indicato, ogni U.O. è responsabile per l'esecuzione delle fasi del processo ad essa attribuite.

Nel caso specifico delle procedure di acquisizione tramite convenzioni CONSIP, la valutazione di conformità deve essere effettuata sulla documentazione disponibile (Guida alla Convenzione, relativi allegati e tutta la documentazione ritenuta utile ai fini dell'analisi di conformità alla normativa sulla Protezione dei Dati e valutazione dei rischi per i diritti e le libertà degli interessati) prima di procedere con l'attivazione della convenzione stessa. Nel caso in cui la valutazione di conformità non avesse esito positivo, sarà necessario identificare una modalità alternativa di acquisizione relativa ad un lavoro, prodotto o servizio equivalente che rispetti i requisiti di conformità normativa e preveda l'adozione di adeguate misure di sicurezza.

In caso di rinnovo di servizio/fornitura da parte della UOC/UOSD/Struttura richiedente, rivolta alla UOC A.B.S., quest'ultima procederà con le stesse modalità previste in caso di richieste di servizio/fornitura che dovessero pervenire per la prima volta.

Nel caso in cui la ASL di Pescara non fosse capofila nell'ambito di una procedura di acquisizione a livello regionale, la UOC ABS dovrà esplicitamente richiedere, per opportuna valutazione di conformità, copia della documentazione di gara per opportuna integrazione.

I documenti prodotti dall'Ufficio Privacy/Protezione dei Dati Personali, a seguito della comunicazione da parte della UOC ABS, nell'ambito della definizione della documentazione per una procedura di acquisizione, sono i seguenti:

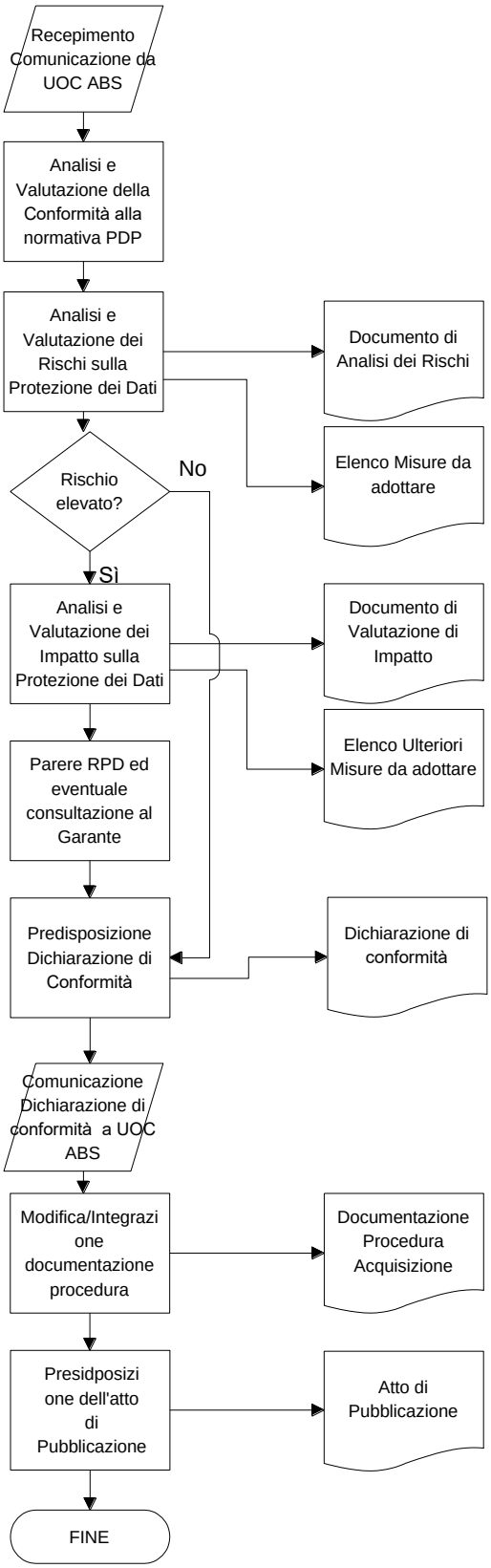
- Documento di Valutazione dei Rischi
- Elenco delle Misure di Sicurezza e degli adempimenti individuati

Nel caso in cui si renda necessaria una Valutazione di Impatto sulla Protezione dei Dati Personali, verranno prodotti i seguenti ulteriori documenti:

- Documento di Valutazione di Impatto sulla Protezione dei Dati Personali
- Elenco delle ulteriori Misure di Sicurezza e adempimenti

Al fine di riepilogare le disposizioni relative agli adempimenti ed alle misure di sicurezza individuate, l'Ufficio Privacy/Protezione Dati Personali dovrà predisporre un opportuno modello di Dichiarazione di Conformità (DC) che dovrà essere comunicato alla UOC ABS per l'inclusione all'interno della documentazione di gara.

Un flusso riepilogativo di tali documenti e relative comunicazioni all'UOC ABS è illustrato nello schema alla pagina seguente:


Recepimento Comunicazione da UOC ABS
Analisi e Valutazione della Conformità alla normativa PDP
Analisi e Valutazione dei Rischi sulla Protezione dei Dati
Documento di Analisi dei Rischi
Elenco Misure da adottare
Rischio elevato?
No
Sì
Analisi e Valutazione dei Impatto sulla Protezione dei Dati
Documento di Valutazione di Impatto
Elenco Ulteriori Misure da adottare
Parere RPD ed eventuale consultazione al Garante
Predisposizione Dichiarazione di Conformità
Dichiarazione di conformità
Comunicazione Dichiarazione di conformità a UOC ABS
Modifica/Integrazione documentazione procedura
Documentazione Procedura Acquisizione
Presidposizione dell'atto di Pubblicazione
Atto di Pubblicazione
FINE

## 6.2 Fase 2: Dichiarazione di conformità ai requisiti individuati in fase 1 e relativa verifica

In base alle varie modalità di acquisizione possibili, secondo quanto previsto dal D. Lgs. 50/2016 e ss.mm.ii. e da tutta la normativa applicabile in materia, la valutazione della rispondenza ai requisiti (adempimenti e misure di sicurezza) inclusi nella documentazione di gara/acquisizione avverrà mediante verifica, da parte del Responsabile Unico del Procedimento designato (RUP), della Dichiarazione di Conformità (DC) debitamente compilata e sottoscritta dal fornitore.

In caso di acquisizione tramite procedura CONSIP la valutazione dovrà essere effettuata dall'Ufficio Privacy/Protezione Dati Personali in Fase 1.

Successivamente alla fase di valutazione, l'Ufficio Privacy/Protezione Dati Personali predisporrà l'Accordo sulla Protezione dei Dati (es.: atto di designazione del Responsabile del Trattamento) ed eventuali allegati da far sottoscrivere al fornitore contestualmente alla firma del contratto.

## 6.3 Fase 3: Validazione operativa della conformità del lavoro, servizio o fornitura

La fase conclusiva del processo di acquisizione è costituita dalla fase di validazione operativa del lavoro, servizio o fornitura rispetto ai requisiti indicati nella documentazione di gara la cui soddisfazione è stata attestata, da parte del fornitore, nella Dichiarazione di Conformità.

Successivamente alla sottoscrizione del contratto, il referente incaricato per la validazione del lavoro, servizio o fornitura (es.: RUP o DEC) è tenuto a contattare l'Ufficio Privacy/Protezione dei Dati Personali per determinare il piano di audit (iniziale e periodico), le modalità di esecuzione ed i soggetti incaricati al fine di effettuare la validazione operativa di conformità rispetto a quanto indicato dal fornitore nella DC.

## 6.4 Responsabilità

La responsabilità della corretta applicazione della presente Procedura è demandata alle funzioni aziendali per la fase attuativa di propria competenza.