Sistema Socio Sanitario
Regione Lombardia
ASST Valtellina e Alto Lario

Direzione amministrativa

PROCEDURA

Procedura per la corretta individuazione, nei contratti e nelle convenzioni, di situazioni di Titolarità autonoma ex art. 24 GDPR, di Contitolarità ex art. 26 GDPR o di nomina di Responsabili e sub-responsabili ex art. 28 GDPR.

INDICE di REVISIONE	00	
DATA di AGGIORNAMENTO	15/11/2022	
DESCRIZIONE MODIFICHE INTEGRAZIONI	Emissione	
FASE	**NOMINATIVO**	**FIRMA**
REDAZIONE Data _____	S. Ruffoni – Ufficio Privacy	
PRE-VERIFICA Data _____	C. Paganoni – Incarico di Organizzazione Qualità e Risk Management - UOC Programmazione Strategica Risk Management e Qualità	
	A. Faccinelli - UOC Programmazione Strategica Risk Management e Qualità	
VERIFICA Data _____	R. Coppola - DPO aziendale	
	S. Benedetti - Responsabile UOS Trasparenza e Internal Auditing	
	R. Paroli - Direttore UOC Approvvigionamenti	
	C. Zanesi - Direttore UOC Gestione Patrimonio Immobiliare	
	A. Panese - Direttore UOC Sistemi Informativi Aziendali	
	C. Cecchini – Responsabile UOS Tecnologie Innovative	
	E. Piazzola - Avvocatura	
APPROVAZIONE Data _____	A. De Vitis - Direttore ad interim UOC Legale, Giuridico e Affari Generali	

VISTO Data _____	A. De Vitis - Direttore Amministrativo	

INDICE

1- Scopo

Il presente documento ha lo scopo di costituire una Linea Guida per la corretta individuazione di situazioni di titolarità autonoma ex art. 24 GDPR, di Contitolarità ex art. 26 GDPR o di nomina di Responsabili e sub-responsabili ex art. 28 GDPR, e di supportare le Strutture Amministrative, Tecniche e Professionali, che gestiscono procedure di appalto e/o convenzioni e/o contratti:

- nella comprensione dei criteri di identificazione delle figure sopra elencate;
- nella gestione sotto il profilo "privacy" dei rapporti contrattuali tra l'ASST e le figure sopra elencate, mediante l'aggiornamento di modelli predefiniti e standardizzati.

2 - Campo di applicazione

I concetti di Titolare del trattamento, Contitolare del trattamento e Responsabile esterno ex art. 28 GDPR sono fondamentali nell'applicazione del Regolamento generale sulla protezione dei dati 2016/679 (GDPR).

La corretta individuazione di tali figure, infatti, assume un ruolo cruciale per la tenuta e l'efficienza del "Sistema privacy" dell'Azienda, determinando chi è responsabile per il rispetto delle diverse norme sulla protezione dei dati e il modo in cui gli interessati possono esercitare i propri diritti nel concreto.

3 - Responsabilità

La responsabilità di aggiornamento della presente procedura e la responsabilità di diffusione sono in capo all'Ufficio Privacy – UOC Legale, Giuridico e Affari Generali.

La responsabilità di applicazione è in capo alla UOC Legale, Giuridico e Affari Generali, alla UOC Approvvigionamenti, alla UOC Gestione Patrimonio Immobiliare, UOC Sistemi Informativi Aziendali e alla UOS Tecnologie Innovative.

4 - Riferimenti normativi

- L. 241/1990 e s.m.i. Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- D. Lgs. 196/2003 e s.m.i. Codice in materia di protezione dei dati personali;
- Regolamento generale sulla protezione dei dati 2016/679 (GDPR)

5- Documenti aziendali di riferimento

Modulo 00 – Mod DA 64 "Atto di nomina a responsabile del trattamento ex art. 28 GDPR per appalti/convenzioni che non implicano particolari rischi nel trattamento dei dati personali";

Modulo 00 – Mod DA 84 "Atto di nomina a responsabile del trattamento ex art. 28 GDPR per appalti/convenzioni che implicano impatti rilevanti al trattamento dei dati personali".

6 - Glossario e Siglario

6.1 Glossario

Il Glossario di riferimento è prioritariamente riconducibile alle definizioni di cui all'art. 4 GDPR, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, che, in caso di discordanza, prevale sul seguente glossario.

- ✓ **Amministratori di Sistema**: figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del provvedimento del 27 novembre 2008 del Garante vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi

relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

- ✓ **Contitolare**: Titolare che determina congiuntamente con altro/i Titolare/i le finalità ed i mezzi del trattamento.
- ✓ **Dato Personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile una persona fisica che può essere identificata direttamente o anche indirettamente, con particolare riferimento ad u identificativo come il nome, un numero 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.
- ✓ **Garante**: l'Autorità Garante per la Protezione dei Dati Personali (GPDP).
- ✓ **Autorizzato o Incaricato:** la persona fisica autorizzata a compiere operazioni di Trattamento su Dati Personali, in virtù delle istruzioni impartite dal Titolare o dai Responsabili.
- ✓ **Interessato**: la persona fisica cui si riferiscono i Dati Personali (tra i quali, a titolo esemplificativo, i pazienti, i dipendenti, i candidati all'assunzione, i fornitori, i visitatori etc.).
- ✓ **Leggi Applicabili**: la normativa europea normativa europea direttamente applicabile negli Stati membri, la normativa nazionale, i provvedimenti del Garante.
- ✓ **Modello Organizzativo Data Protection**: documento composto da una prima sezione denominata "Principi generali e modello organizzativo" in cui sono esposti i principi generali che regolano le attività di trattamento di dati personali eseguite dall'Azienda, le figure del sistema privacy e l'organigramma privacy dei responsabili interni e da una seconda sezione denominata "Modello di Gestione" composta da una molteplicità di documenti riguardanti la metodologia di gestione dell'attività di trattamento e di protezione dei dati persone delle persone fisiche.
- ✓ **Regolamento Europeo:** il Regolamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei Dati Personali, nonché alla libera circolazione di tali dati, entrato in vigore il 24 maggio 2016 e direttamente applicabile in tutti i Paesi UE a decorrere dal 25 maggio 2018.
- ✓ **Responsabile del trattamento**: la Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare.
- ✓ **Responsabile interno del trattamento:** soggetto espressamene designato, a sensi dell'art. 2 quaterdecies del D. Lgs. 196/2003 e s.m.i., dal Titolare o dal Responsabile, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, a svolgere determinati compiti o funzioni connesse al trattamento di dati personali.
- ✓ **Responsabile della Protezione dei Dati (DPO o RDP):** soggetto nominato dal Titolare o dal Responsabile del Trattamento in funzione delle qualità professionali e in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti indicati dall'art. 39 del Regolamento Europeo.
- ✓ **Sistema Privacy:** complesso della documentazione (ivi inclusi i documenti propriamente afferenti al Modello Organizzativo Data Protection) e delle prassi in essere riguardanti il trattamento e la protezione dei dati personali delle persone fisiche.

- ✓ **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.
- ✓ **Titolare:** la persona fisica o persona giuridica, l'autorità pubblica, il servizio o altro organismo che singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di Dati Personali.
- ✓ **Trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insieme 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.

6.2 Siglario

- GDPR: General Data Protection Regulation.
- GPDP: Autorità Garante per la Protezione dei Dati Personali.
- ASST: Azienda Socio Sanitaria Territoriale
- MODP: Modello Organizzativo Data Protection
- UP: Ufficio Privacy
- DPO: Data Protection Officer
- Gruppo WP29: Gruppo di lavoro gruppo di lavoro europeo (cessato il 25.05.2018)
- EDPB: European Data Protection Board
- RDP: Responsabile della Protezione dei Dati
- U.O.C.: Unità Organizzativa Complessa
- U.O.S.: Unità Organizzativa Semplice Struttura
- SEE: Spazio Economico Europeo
- SGQ: Sistema di Gestione Qualità
- UE: Unione Europea

7 - Descrizione delle attività.

Le prescrizioni di seguito dettagliate sono finalizzate a regolamentare le ipotesi di titolarità autonoma ex art. 24, di Contitolarità ex art. 26 o di nomina di Responsabili e sub-responsabili ex art. 28. Fattispecie sostanzialmente diverse ma caratterizzate da un elemento comune, ovvero il sottendere un trattamento di dati personali come definito al par. 2.1 della presente procedura.
Esulano, pertanto, dall'ambito applicativo del presente documento esclusivamente gli accordi convenzionali/gli appalti che ***non*** prevedono per la loro esecuzione il trattamento di dati riferibili a persone identificate o identificabili.

7.1 - Situazioni di Titolarità autonoma (Titolare – Titolare) ex art. 24 GDPR.

7.1.1 - Criteri di individuazione.

Il Titolare del trattamento è colui che determina in modo autonomo ed esclusivo le finalità e i mezzi del trattamento. Titolare è sempre l'organizzazione in quanto tale e non un individuo all'interno dell'organizzazione.

7.1.2 - Modalità di formalizzazione: modello di clausola.

Nel caso in cui la contro-parte contrattuale assuma il ruolo di Titolare "autonomo" del trattamento" (ossia quando definisce in modo autonomo ed esclusivo le modalità e finalità del trattamento), occorre individuare fin dalla fase istruttoria (ad esempio nella bozza contratto) la clausola contrattuale che disciplinerà i rapporti tra le parti in materia di "trattamento dati" e che dovrà poi essere recepita nell'accordo sottoscritto.

La situazione di "titolarità autonoma" riguarda, normalmente, ambiti di attività che trovano la propria cornice giuridica all'interno di accordi di tipo "convenzionale". La situazione in oggetto ricorre, a titolo esemplificativo, nell'ambito dei bandi di gara per l'affidamento dei servizi assicurativi.

A titolo di ausilio sono state tuttavia predisposte due diverse clausole contrattuali "tipo": una per convenzioni e un'altra per appalti, dal contenuto sovrapponibile:

- Modello di *clausola* in situazioni di **titolarità autonoma** (Titolare - Titolare) ex art. 24 GDPR **(Appalti)** (allegato n. 1)
- Modello di *clausola* in situazioni di **titolarità autonoma** (Titolare - Titolare) ex art. 24 GDPR - **(Accordi/Convenzioni)** (allegato n. 2)

7.2 - Situazioni di Contitolarità ex art. 26 GDPR.

7.2.1 - Criteri di individuazione.

La qualifica di contitolari del trattamento è attribuita quando più di un Titolare è coinvolto nel trattamento e tutti i Titolari concorrono nella determinazione delle finalità e dei mezzi di un'operazione di trattamento. Il criterio generale per l'esistenza della situazione di "Contitolarità" è pertanto costituito dalla partecipazione congiunta di due o più soggetti alla determinazione delle finalità e dei mezzi di un'operazione di trattamento. Può essere utile evidenziare che l'art. 26 GDPR nel definire la contitolarità utilizza l'espressione specifica "determinare" e non semplicemente "condividere".
La suddetta determinazione congiunta di finalità e mezzi del trattamento può assumere la forma di una decisione assunta in comune da due o più entità o derivare da decisioni convergenti di due o più entità, ovvero da decisioni che si completano a vicenda e sono necessarie in egual modo affinché il trattamento possa accadere.
A tal riguardo ed in via meramente esemplificativa, si precisa che – come affermato in un'opinione del Gruppo WP29 – si possono configurare (almeno) due forme di contitolarità:

- una contitolarità piena, quando vi è definizione congiunta di tutte le finalità e di tutti i mezzi impiegati;
- una contitolarità parziale, quando le parti definiscono congiuntamente solo una parte delle finalità o dei mezzi.

Nel caso in cui l'Azienda condivida la determinazione in merito alle finalità e ai mezzi del trattamento con altri soggetti questi ultimi, pertanto, assumono la posizione di ***Contitolari del trattamento.***

La situazione di "Contitolarità" è rara e riguarda, normalmente, ambiti di attività che trovano la propria cornice giuridica in accordi di tipo "convenzionale". La situazione in oggetto ricorre, a titolo esemplificativo, nelle ipotesi di accordi atti a disciplinare attività di tirocinio universitario, scuole di specializzazione, prestazioni socio-sanitarie erogate congiuntamente ad altri enti del SSN, etc.

7.2.2 - Modalità di formalizzazione.

La situazione di "Contitolarità" è quindi correlata a particolari accordi che, al di là del "*nomen iuris*" e dell'oggetto dell'accordo principale richiedono necessariamente, per essere attuati, una "determinazione congiunta" sulle finalità e sui mezzi del trattamento dei dati di persone fisiche.

Tutte le situazioni di contitolarità sono infatti formalmente disciplinate attraverso appositi accordi, in cui trovano puntuale esplicazione e definizione i ruoli reciproci e il riparto degli obblighi. Gli accordi di contitolarità, una volta concordati con l'altra parte contraente (Contitolare), sono allegati all'accordo/convenzione/contratto "principale" quale parte integrante e sostanziale dello stesso per la necessaria sottoscrizione.

Nel caso in cui la contro-parte contrattuale e l'ASST assumano il ruolo di "Contitolari" del trattamento (ossia quando determinino congiuntamente le finalità e i mezzi del trattamento), occorre finalizzare le attività istruttorie ai seguenti obiettivi:

- ✓ inserimento nel contratto/convenzione principale di una "clausola contrattuale" che rinvii specificatamente ad un accordo di contitolarità;
- ✓ stipulazione di un accordo di contitolarità;
- ✓ predisposizione di un'informativa ex art. 13 GDPR *ad hoc* da rendere agli Interessati al momento di avvio del trattamento;
- ✓ definizione delle modalità di diffusione e comunicazione dell'estratto dell'accordo di contitolarità formalizzato tra le parti;
- ✓ registrazione della contitolarità all'interno del Registro dei trattamenti ex art. 30 GDPR.

A titolo di ausilio sono stati predisposti due modelli: uno per la clausola contrattuale (da inserire nel testo dell'accordo/contratto/convenzione "principale") ed uno per l'accordo di Contitolarità (da allegare all'accordo/contratto/convenzione "principale"). In particolare:

- Modello di *clausola* in situazioni di **Contitolarità** ex art. 26 GDPR **(Appalti/Convenzioni)** - (allegato n. 3).
- Modello di *accordo/contratto* in situazioni di **Contitolarità** ex art. 26 GDPR **(Appalti/Convenzioni)** - (allegato n. 4)

N.B. È opportuno che la sottoscrizione di Accordi di Contitolarità differenti rispetto al format allegato alla presente procedura sia sottoposto preliminarmente alla verifica ed alla approvazione del DPO aziendale che, pertanto, deve essere interpellato da parte della Struttura proponente per tempo e fin dalla fase istruttoria.

7.3 - Situazioni di Responsabilità ex art. 28 GDPR

7.3.1 - Criteri di individuazione.

La qualifica di Responsabile ("esterno") del trattamento ex art. 28 GDPR è attribuita ad una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che tratta dati personali per conto del Titolare (art. 4, pf. 8 GDPR).
I criteri fondamentali per l'individuazione del Responsabile, pertanto, sono i seguenti:

- ✓ che sia un'entità distinta e separata rispetto al Titolare del trattamento;
- ✓ che tratti dati personali per conto del Titolare del trattamento e su sua documentata istruzione (fermo restando che le istruzioni del Titolare del trattamento possono lasciare un certo grado di discrezionalità consentendo al responsabile del trattamento di scegliere la soluzione tecnica e organizzativa più adatta al caso concreto).

N.B. il fatto che il Responsabile ("esterno") sia tenuto a trattare dati per conto del Titolare implica necessariamente che il medesimo entri a far parte del "Sistema privacy" dell'ASST e, di conseguenza,

sia tenuto a trattare i dati secondo le istruzioni del Titolare (soggetto che determina finalità e mezzi del trattamento - vedi sopra punto 3.1).

Si evidenzia infine che la nomina del Responsabile ex art. 28 costituisce la fattispecie più comune e diffusa nell'ambito della cornice giuridica dei contratti di appalto e, in generale, nell'ambito accordi che, al di là del *nomen iuris*, comportino la necessità, per essere attuati, di trattare dati personali di persone fisiche per conto del Titolare/ASST della Valtellina e dell'Alto Lario.
La situazione in oggetto ricorre, a titolo esemplificativo, nelle ipotesi di forniture di sistemi ed applicativi informatici, acquisto di dispositivi elettromedicali e di correlati servizi di assistenza e manutenzione, affidamento a terzi delle attività di prenotazione e gestione delle agende, affidamento a terzi delle attività di trasporto di pazienti e/o di documentazione afferente allo stato di salute degli utenti, coinvolgimento di associazioni di volontariato o enti di pari natura nelle attività di assistenza e supporto al paziente e/o ai suoi familiari, affidamento a terzi delle attività di controllo sugli accessi correlati all'emergenza sanitaria da Covid19, etc.

7.3.2 - Modalità di formalizzazione.

OBIETTIVI:
Nel caso in cui la contro-parte contrattuale assuma il ruolo di "Responsabile del trattamento ex art. 28 GDPR" (ossia quando essa è tenuta e trattare dati per conto del Titolare/ASST della Valtellina e dell'Alto Lario) occorre finalizzare le attività istruttorie ai seguenti obiettivi:

- ✓ inserimento nello schema di capitolato/contratto/convenzione di una "clausola contrattuale" che rinvii specificatamente ad un atto (*rectius* – "contratto") di nomina del Responsabile ("esterno") del trattamento ex art. 28 GDPR;
- ✓ definizione ed utilizzo di uno strumento di assessment finalizzato ad accertare la sussistenza di un livello minimo di compliance del soggetto terzo alla normativa, europea e nazionale, in materia di protezione dei dati personali delle persone fisiche;
- ✓ inserire/allegare allo schema di capitolato/contratto uno schema di atto (*rectius* "contratto") di nomina del Responsabile ("esterno") ex art. 28 GDPR, che dopo l'aggiudicazione sarà oggetto di stipulazione quale parte integrante e sostanziale del contratto principale;
- ✓ registrazione della nomina del responsabile ("esterno") ex art. 28 GDPR.

STRUMENTI:
A tale scopo ed a titolo di ausilio sono stati predisposti i seguenti modelli:

- Modello di *clausola* contrattuale per la nomina di **Responsabili (esterni) ex art. 28 GDPR**:
  - Per Appalti - da inserire nello schema di capitolato/contratto e che rinvia specificatamente ad un atto (rectius – "contratto") di nomina del Responsabile ("esterno") del trattamento ex art. 28 GDPR - (allegato 5);
  - Per Convenzioni - da inserire nella convenzione e che rinvia specificatamente ad un atto (rectius – "contratto") di nomina del Responsabile ("esterno") del trattamento ex art. 28 GDPR - (allegato 6);
- *Un Questionario di 1° livello* comune a tutte le procedure che effettuano un trattamento di dati personali per verificare la sussistenza di un livello minimo di "compliance" al GDPR, da inserire tra i documenti che debbono essere prodotti nella documentazione amministrativa, da parte dei soggetti che partecipano alle procedure di gara (ovvero che debbono essere prodotti dal soggetto interessato a stipulare una Convenzione) – (Allegato 7).

- Il Modello di atto di nomina dei Responsabili (esterni) ex art. 28 GDPR (Appalti e Convenzioni) viene inserito nel capitolato/contratto e, pertanto, sarà oggetto di espressa accettazione da parte di tutti i soggetti partecipanti alla gara, in analogia a tutte le altre clausole contrattuali e secondo le normali procedure aziendali. Il Modello si presta a due differenti livelli di applicazione:
    - per le procedure relative ad attività che non implicano particolari rischi nel trattamento dei dati delle persone fisiche è sufficiente utilizzare l'allegato 8.
    - nelle sole ipotesi in cui il servizio oggetto di procedura abbia impatti rilevanti sul trattamento di dati personali (ad esempio utilizzo/acquisto applicativi informatici che trattano dati personali di persone fisiche) sarà necessario utilizzare l'allegato 9, specificatamente predisposto per la qualifica di Responsabili che dovranno effettuare tali trattamenti. Il Modello (allegato 9) non è rigido e pertanto, in caso di dispositivi o applicativi informatici particolarmente invasivi, l'UOC SIA potrà essere coinvolto per la verifica del contenuto dell'Allegato B del Modello e successivamente per il supporto durante la fase di preparazione al capitolato di gara.
- Un Modello di Registro/Elenco dei Responsabili ex art. 28 GDPR – (cfr. infra punto 3.5)

PROCEDURA:

Il Capitolato tecnico – predisposto dal Servizio / Struttura richiedente ed eventualmente condiviso con UOC SIA - è trasmesso alla U.O.C. Approvvigionamenti per la predisposizione della documentazione di gara.

Nella fase preparatoria di una procedura di gara per l'acquisto di una fornitura o di un servizio, il Servizio Approvvigionamenti invia alle ditte interessate alla Procedura di Acquisto un Questionario di 1° livello e comune a tutte le procedure, al fine di accertare mediante la compilazione del questionario stesso ed alla produzione della relativa autocertificazione se la ditta offerente per tramite del prodotto offerto effettui un trattamento di dati personali e per verificare la sussistenza di un livello minimo di "compliance" al GDPR. Questa documentazione farà parte integrante della successiva documentazione Amministrativa di gara e sarà oggetto di valutazione ai fini del possesso dei requisisti della ditta offerente.

Successivamente potrà essere inviata una richiesta motivata all'U.O.C. SIA per verificare eventuali aspetti di cybersecurity e per l'eventuale nomina degli amministratori di sistema e/o una richiesta motivata al DPO (o al suo team) per verificare i profili "privacy". Tali supporti sono facoltativi e le richieste devono essere motivate e supportate da coerente documentazione.

In particolare:

- Il Modello di *clausola* per nomina di Responsabili (esterni) ex art. 28 GDPR (– allegato 5 - oppure– allegato 6) viene inserito nello schema di capitolato generale d'appalto/contratto e, pertanto, sarà oggetto di espressa accettazione da parte di tutti i soggetti partecipanti alla gara, in analogia a tutte le altre clausole contrattuali e secondo le normali procedure aziendali. Analogamente si procede anche per le Convenzioni.
- Il Questionario di 1° livello (Allegato 7) per verificare la sussistenza di un livello minimo di *"compliance"* al GDPR viene previsto nella procedura di gara d'appalto tra i documenti che debbono essere prodotti come "documentazione amministrativa" e che devono essere valutati, da parte del seggio di gara, ai fini dell'ammissibilità del soggetto partecipante. Infatti in ogni ipotesi in cui l'attività oggetto del bando di gara comporti direttamente o indirettamente il trattamento di dati personali di Interessati soggetti alla titolarità dell'ASST, l'adeguatezza del

soggetto terzo che sottopone la propria offerta all'ASST deve essere valutata attraverso una check list ("Questionario di assessment di 1°livello"). La suddetta check list consente, di formulare in forma automatizzata un giudizio sul livello di compliance del soggetto terzo. La valutazione e l'accertamento del possesso di un livello minimo di compliance avviene, sulla base delle autocertificazioni del soggetto terzo, in modo automatico e trasparente sulla base di criteri predefiniti. L'ottenimento di un punteggio pari o superiore a 5 costituisce condizione di ammissione alle fasi successive della procedura di gara.

- A tal riguardo, si precisa che nei casi in cui si renda necessaria un'attività di verifica della documentazione presentata, anche mediante richiesta di chiarimenti o elementi integrativi, per il tramite del c.d. soccorso istruttorio ai sensi dell'art. 83 del D.Lgs. 50/2016, la U.O.C. Approvvigionamenti provvederà all'ammissione con riserva dei concorrenti interessati e analizzerà i riscontri pervenuti con il supporto tecnico del DPO.
- Il Modello di atto di nomina di Responsabili (esterni) ex art. 28 GDPR (Appalti e Convenzioni) - (allegato 8 e allegato 9), precompilato (nella tabella "Tabella - Elementi essenziali del trattamento") dalla Struttura Richiedente (vedi sopra), è previsto nella procedura di gara d'appalto tra i documenti che debbono essere prodotti dal soggetto partecipante in sede di "offerta" e che potranno essere valutati ai fini della scelta del contraente. Analogamente si procede anche per le Convenzioni.

Il Modello non è rigido e pertanto, in caso di dispositivi o applicativi informatici particolarmente invasivi, può anche essere implementato nella fase di progettazione e di preparazione del capitolato di gara, coinvolgendo l'U.O.C. SIA per la verifica del contenuto del Modello su richiesta della Struttura Richiedente o anche dall'U.O.C. Approvvigionamenti.

Si evidenzia che l'allegato 8 differisce dall'allegato 9 unicamente per l'ampiezza dell'autocertificazione relativa alle misure tecniche ed organizzative adottate dal soggetto partecipante/Responsabile in materia di protezione dei dati personali delle persone fisiche.
Non si differenzia invece il possibile utilizzo dei due modelli nell'ambito delle procedure di scelta del contraente.
Entrambi infatti possono essere utilizzati per valutare l'offerta dei soggetti partecipanti alla procedura di selezione secondo le modalità che, di volta in volta, verranno ritenute più opportune ed adeguate da parte delle Strutture deputate alla elaborazione ed alla approvazione della procedura di gara e del capitolato di gara.
In via meramente esemplificativa: l'esito della valutazione può essere considerato rilevante ai fini della scelta del contraente unicamente nel caso in cui due o più concorrenti conseguano il medesimo punteggio tecnico/economico. In alternativa l'esito della valutazione può incidere nell'attribuzione del punteggio secondo la parametrazione che verrà ritenuta più opportuna ed adeguata da parte delle Strutture deputate alla elaborazione ed alla approvazione della procedura di gara e del capitolato di gara.

Esperita la procedura di affidamento dell'appalto (o di condivisione dello schema di convenzione) gli atti di nomina del Responsabile ex art. 28 GDPR, già compilati e accettati dall'aggiudicatario, sono allegati all'accordo/convenzione/contratto "principale" ed approvati mediante il provvedimento amministrativo di aggiudicazione dell'appalto.

Con il provvedimento di aggiudicazione si cristallizza la documentazione contrattuale da sottoscrivere tra le Parti e l'atto (rectius "contratto") di nomina del Responsabile ("esterno") ex art. 28 GDPR che costituisce ad ogni conseguente effetto parte integrante e sostanziale del contratto "principale".

Tale assetto contrattuale è insuscettibile di modifiche. Tuttavia nel denegato caso in cui il soggetto aggiudicatario chieda di sottoscrivere un atto di nomina sostanzialmente diverso da quello approvato in

sede di aggiudicazione la U.O.C./U.O.S. che ha la responsabilità del procedimento valuta, preliminarmente, se sussistono i presupposti di legittimità per accogliere tale richiesta e in caso affermativo può avvalersi del supporto del DPO, per i soli profili "privacy", al fine di valutare l'adeguatezza rispetto al GDPR dell'atto di nomina modificato.

La clausola contrattuale, l'atto (rectius "contratto") di nomina con i relativi allegati A) (Elenco dei sub responsabili) e B (misure di protezione, tecniche ed organizzative) compongono il quadro della documentazione che l'ASST, in qualità di Titolare, fornisce fin dal momento di avvio del trattamento al soggetto aggiudicatario/contraente e Responsabile ("esterno") ex art. 28 GDPR.

Qualsiasi trattamento di dati personali da parte di un Responsabile del trattamento deve infatti essere regolato da un contratto o da un altro atto giuridico vincolante, da concludere in forma scritta, anche in formato elettronico.

- Il Modello di Registro/Elenco dei Responsabili ex art. 28 GDPR (cfr. infra punto 3.5) viene compilato dopo la firma del contratto/convenzione e dell'atto di nomina a responsabile ed è conservato a cura della U.O.C./U.O.S. che cura l'istruttoria ex L. 241/1990 e s.m.i., in conformità al M.O.D.P. aziendale.

7.3.3 - Modalità di formalizzazione: quando l'ASST è nominata Responsabile ex art. 28 GDPR.

Quando l'ASST assume il ruolo di Responsabile ex art. 28 GDPR, deve essere nominata Responsabile "esterno" da un altro soggetto Titolare e ricevere le istruzioni, in quanto, in tale caso, deve trattare dati personali di persone fisiche per conto di altro titolare ed entra quindi a far parte del "sistema privacy" di altro Titolare (ad esempio: accordi "attivi" per l'erogazione di prestazioni sanitarie a terzi). In tale caso gli adempimenti dovuti sono opposti a quelli di cui al punto 7.2.2 e, in particolare, sono i seguenti:

- ✓ verificare di aver ricevuto apposita e formale nomina ex art. 28 GDPR;
- ✓ valutare, prima della sottoscrizione della suddetta nomina, che i suoi contenuti siano coerenti con la normativa vigente e con le caratteristiche dell'attività a cui la nomina afferisce;
- ✓ dopo aver sottoscritto la nomina, tracciare il trattamento eseguito in nome e per contro di terzi nell'apposito Registro ex art. 30 par. 2 GDPR.

7.4 - Registro/Elenco dei Responsabili ex art. 28 GDPR

Gli accordi di contitolarità stipulati (normalmente sottoscritti con altri Enti pubblici a corredo e completamento di rapporti contrattuali o convenzionali che regolano servizi o attività di cui si condividono le finalità), gli atti di nomina dei Responsabili esterni e l'elenco dei Responsabili del trattamento ex art. 28 GDPR sono compilati/registrati e conservati presso ciascuna U.O.C./U.O.S. che cura la relativa istruttoria ex Legge n. 241/1990 e s.m.i..

Per la registrazione e la conservazione degli elenchi da parte delle Strutture che curano l'istruttoria ex L. 241/1990 e s.m.i. è predisposto, a mero titolo di ausilio, un "format" in Excel denominato "Modello di Registro/Elenco dei Responsabili ex art. 28 GDPR" - (allegato n.10).

7.5 - Trasferimento dati extra SEE.

Ai sensi e per gli effetti di cui all'art. 44 GDPR qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, (ossia extra UE) ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni previste al capo V del citato regolamento europeo, finalizzate ad assicurare che il livello di protezione delle persone fisiche garantito dal regolamento stesso non sia pregiudicato.

Tale normativa implica una particolare e rigorosa attenzione del Titolare verso il rischio di trattamenti extra UE, soggetti a norme specifiche e stringenti.
A tale scopo la modulistica allegata alla presente procedura è idonea anche a rilevare, sin dalla fase istruttoria, se il Responsabile ex art. 28 GDPR, che tratta dati per conto del Titolare/ASST, trasferisce o tratta dati al di fuori della U.E.
In caso di trasferimento di dati verso un Paese terzo o una organizzazione internazionale, fatte salve le ipotesi in cui il Responsabile debba adempiere ad un obbligo imposto dal diritto UE o dal diritto nazionale, il Responsabile ex art. 28 dovrà richiedere espressa e specifica autorizzazione all'ASST/Titolare del trattamento, garantire che il trasferimento avvenga in sussistenza di almeno una delle condizioni di legittimità previste dal GDPR dimostrando che il livello di protezione degli interessati non sia pregiudicato rispetto alle garanzie offerte dal GDPR.
Per la valutazione di tali situazioni specifiche i Direttori delle Strutture Amministrative, Tecniche e Professionali interessate potranno avvalersi del supporto del DPO aziendale.

In tale contesto è opportuno evidenziare che i principi generali sopra succintamente esposti valgono anche nei confronti degli U.S.A.
Nello specifico la Corte di Giustizia Europea è intervenuta il 16 luglio 2020 - sentenza Schrems II - in materia di trasferimento di dati personali verso gli Stati Uniti, invalidando il c.d. "Privacy Shield" (ovvero un meccanismo di autocertificazione di conformità al GDPR per le società stabilite in USA).
Con la suddetta Sentenza la Corte, in particolare, ha annullato la decisione con cui la Commissione europea aveva adottato il cd. Scudo del Privacy Shield, senza preservarne gli effetti, ed ha ritenuto che le clausole contrattuali "tipo" non sono idonee a garantire un livello di protezione analogo a quello assicurato in Europa dal GDPR.
Allo stato attuale pertanto tutte le società che svolgono trattamenti di dati personali di cittadini europei o per conto di società europee all'interno del territorio degli Stati Uniti sono tenute ad individuare un presupposto giuridico diverso dal c.d. Privacy Shield per il trasferimento di dati.

7.6 - Accordi che non prevedono trattamento di dati personali

In caso di accordi convenzionali/gli appalti che non prevedono per la loro esecuzione il trattamento di dati riferibili a persone identificate o identificabili, nell'accordo sottoscritto dalle parti potrà essere inserito il Modello di clausola informativa di cui all'Allegato "Modello di Clausola tipo in situazioni in cui non è previsto trattamento di dati personali". (Allegato n.11).

8 - Allegati

1. Modello di *clausola* in situazioni di titolarità autonoma (**Titolare- Titolare**) ex art. 24 GDPR (**Appalti**).
2. Modello di *clausola* in situazioni di titolarità autonoma (**Titolare- Titolare**) ex art. 24 GDPR (**Convenzioni**).
3. Modello di *clausola* in situazioni di **Contitolarità** ex art. 26 GDPR (**Appalti/Convenzioni**).
4. Modello di *accordo/contratto* in situazioni di **Contitolarità** ex art. 26 GDPR (**Appalti/Convenzioni**).
5. Modello di *clausola* per nomina di **Responsabili** (esterni) ex art. 28 GDPR (**Appalti**).
6. Modello di *clausola* per nomina di **Responsabili** (esterni) ex art. 28 GDPR (**Convenzioni**).
7. Check list per verificare la sussistenza di un livello minimo di "compliance" al GDPR.
8. Modello di Re**gistro/Elenco** dei **Responsabili** ex art. 28 GDPR.
9. Modello di Clausola tipo in situazioni in cui non è previsto trattamento di dati personali.