PROCEDURA PER LA NOMINA DEI RESPONSABILI ESTERNI

Autori:	Dott.ssa Alessia Cifaldi Dott. Giuseppe Napolitano Dott.ssa Francesca Esempio	**UOS Privacy**
Approvato da:	Avv. Stefano Rotondo	**DPO ASL Napoli 3 SUD**
Adottato da:	Dott. Giuseppe Russo	**Direttore Generale ASL Napoli 3 Sud**

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autori**
1.0	11/2024	Prima versione	Dott.ssa Alessia Cifaldi Dott. Giuseppe Napolitano Dott.ssa Francesca Esempio UOS Privacy
L'ultima revisione sostituisce qualsiasi revisione precedente.			

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
TEL 081/8490645- PROTOCOLLO@PEC.ASLNAPOLI3SUD.IT

PROCEDURA PER LA NOMINA DEI RESPONSABILI ESTERNI

Sommario

Premessa 3
Capitolo 1 – Ambito di applicazione 3
Scopo 3
Applicabilità 3
Supporto fornito dal DPO 3
Capitolo 2 – Definizioni e norme di riferimento 4
Acronimi e abbreviazioni 4
Definizioni 4
Normativa di riferimento 6
Capitolo 3 – Gestione dei rapporti tra il Titolare ed i responsabili esterni del trattamento 7
Il responsabile esterno del trattamento: Ruolo e gestione dei rapporti 7
Procedura per la designazione dei responsabili del trattamento 8
Workflow riepilogativo del processo di nomina del Responsabile esterno 10
Revisione dei contratti in essere 11
Canali di comunicazione 11
Eventuale designazione di sub-responsabili 12
Capitolo 4 – Gestione dei dati personali oggetto di trattamento 13
Individuazione dei trattamenti e dei dati personali affidati ai responsabili 13
Gestione delle informative agli interessati 13
Gestione degli adempimenti per l'esercizio dei diritti dell'interessato 14
Gestione delle violazioni della sicurezza dei dati personali 14
Gestione delle verifiche svolte dal Titolare 14
Disposizioni finali 14
Capitolo 6 – Allegati 15
Documenti allegati 15

PREMESSA

Il principio di responsabilizzazione, sancito dal Regolamento UE 2016/679, di seguito GDPR o Regolamento, attribuisce all'Azienda Sanitaria Locale Napoli 3 Sud (d'ora in avanti "Titolare del trattamento" o, più semplicemente, "Titolare"), la piena responsabilità nel porre in atto tutte le misure necessarie a garantire il rispetto dei diritti dell'Interessato e un'adeguata sicurezza dei dati personali, durante tutto il ciclo di vita dei trattamenti. In accordo a questo principio, il Titolare del trattamento risponde anche dell'operato di soggetti esterni che svolgono trattamenti di dati personali per suo conto.

CAPITOLO 1
AMBITO DI APPLICAZIONE

CAP. 1

SCOPO

Questo documento ha lo scopo di regolamentare i rapporti tra il Titolare ed i soggetti esterni, siano esse persone fisiche o giuridiche, che effettuano per conto del Titolare, servizi di qualsiasi natura che comportano un trattamento di dati personali.

Con la presente procedura l'Azienda intende disciplinare le modalità operative interne per la ricognizione, identificazione e formale nomina dei "Responsabili esterni al trattamento dei dati" ai sensi del GDPR n. 679/2016, atteso che la nomina di ciascun Responsabile esterno dei dati verrà disciplinata da apposito contratto, il cui schema è allegato al presente documento, in conformità al comma 3 dell'art.28 del GDPR.

La procedura aziendale per la nomina dei Responsabili esterni al trattamento dei dati stabilisce i contenuti degli accordi tra il Titolare del Trattamento (Data Controller) che intende esternalizzare un trattamento di dati personali e il Responsabile (Data Processor), ossia il soggetto incaricato di detto trattamento (fornitore di servizi o di attività/prestazioni esternalizzati, sia esso un outsourcer tradizionale o un cloud service provider). Pertanto, la presente procedura deve essere applicata già in fase precontrattuale, nell'ambito dell'esternalizzazione di servizi, attività o prestazioni che comportano un trattamento di dati personali. Contestualmente è necessario altresì, verificare, aggiornare ed integrare i contratti già in essere che comportano l'esternalizzazione del trattamento di dati personali. Con la presente policy, il Titolare del trattamento dispone l'attuazione delle misure organizzative e procedurali che assicurino una corretta applicazione degli articoli 24, 28, 79 e 82 del Regolamento.

APPLICABILITÀ

La presente procedura è destinata a tutto il personale che svolge le attività connesse all'instaurazione ed esecuzione dei contratti con i soggetti esterni che effettuano un trattamento di dati personali per conto del Titolare.

SUPPORTO FORNITO DAL DPO

Il supporto fornito dal DPO dell'Azienda Sanitaria Locale Napoli 3 Sud, qualora opportunamente consultato, è improntato alla sensibilizzazione e formazione data protection, come previsto dall'art. 39 del GDPR. Il DPO,

infatti, non può in alcun caso prendere decisioni al posto del Titolare del trattamento o sostituirsi nelle valutazioni rimesse dalla normativa data protection in capo a quest'ultimo.

CAPITOLO 2
DEFINIZIONI E NORME DI RIFERIMENTO

❖ ACRONIMI E ABBREVIAZIONI

DPO	Data Protection Officer – Responsabile della Protezione dei Dati
EDPB	European Data Protection Board – Comitato europeo per la Protezione dei Dati. Organismo europeo indipendente il cui scopo è garantire un'applicazione coerente del GDPR.
ENISA	European Union Agency for Network and Information Security
GDPR	General Data Protection Regulation – Regolamento Generale sulla Protezione dei Dati, n. 2016/679
IT	Information Technology
WP29	Working Group 29: gruppo istituito ai sensi dell'art. 29 della direttiva 95/46 CE. Dal 25 Maggio 2018 prende il nome di European Data Protection Board.

❖ DEFINIZIONI

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 (art. 4, n. 6, GDPR).
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica, anche indiretta, dell'identità dell'utente.
Autorità Garante per la Protezione dei Dati Personali	Autorità istituita dalla legge 31 dicembre 1996, n. 675. Ha sede a Roma.
Banca dati	Qualsiasi complesso organizzato di dati (archivio informatico), riguardanti uno stesso argomento o più argomenti correlati tra loro, strutturato in modo tale da consentire la gestione dei dati stessi (l'inserimento, la ricerca, la cancellazione ed il loro aggiornamento) da parte di un'applicazione, ripartito in uno o più elaboratori elettronici (ad es. server, postazioni lavorative, ecc.) dislocati all'interno della rete LAN del Titolare.
Cancellazione sicura	Modalità di cancellazione che consiste nell'eliminazione irreversibile dei dati contenuti in un supporto elettronico in modo che essi non siano più accessibili a terzi o risultino comunque inintelligibili impedendo così il recupero degli stessi.
Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9, c. 1, GDPR).
Classificazione	L'attribuzione all'informazione di un livello di classificazione ovvero il suo inserimento all'interno di una classe di sicurezza.
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del Titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile.
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 (art. 4, n. 11, GDPR).
Credenziali di autenticazione	I dati ed i dispositivi in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica.
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 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 personali relativi a condanne penali o reati	Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 GDPR).
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 (art. 4, n. 1, GDPR).
Declassificazione	La soppressione di qualsiasi menzione di classificazione.
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.
Diffusione	Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.
Documento cartaceo	L'insieme aggregato di informazioni su supporti cartacei.
Documento elettronico	L'insieme aggregato di informazioni su supporti informatici, ovvero file generati attraverso l'utilizzo delle applicazioni informatiche del Titolare.
Incaricato del trattamento	Persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile.
Informazione	La rappresentazione di dati, atti o fatti rilevanti per il Titolare.
Interessato del trattamento	Persona fisica cui si riferiscono i dati personali.
Minimizzazione dei dati	Ogni Titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento, nel rispetto dei principi di adeguatezza (proporzionalità rispetto alle finalità) e pertinenza dei dati e limitazione dei trattamenti solo per il raggiungimento delle finalità previste.

Parola chiave	Componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
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 (art. 4, n. 5, GDPR).
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 (art. 4, n. 8, GDPR).
Riclassificazione	La ridefinizione del livello di classificazione attribuito all'informazione e, quindi, lo spostamento all'interno di un'altra classe di sicurezza.
Sistema di autorizzazione	L'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.
Sistema informativo	L'insieme di dispositivi, programmi ed infrastruttura di rete.
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 (art. 4, n. 7, GDPR).
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 (art. 4, n. 2, GDPR).
Videosorveglianza	Sistema o dispositivo che permette la visione e la registrazione su supporti singoli, abbinati ad altre fonti o conservati in banche dati di immagini di aree o zone delimitate.
Violazione dei dati personali	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 (art. 4, n. 12, GDPR).

❖ NORMATIVA DI RIFERIMENTO

D.lgs. n. 101/2018	Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (GDPR).
D.lgs. n. 196/2003	Decreto Legislativo n. 196 del 30 giugno 2003, contenente il "Codice in materia di protezione dei dati personali", n. c. "Codice Privacy".
Regolamento UE 2016/679	Regolamento del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).
Legge n. 300/1970	Statuto dei Lavoratori.

Provvedimento n. 467/2018	Provvedimento dell'Autorità Garante della Protezione dei Dati Personali n. 467 dell'11 ottobre 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".

CAPITOLO 3
GESTIONE DEI RAPPORTI TRA IL TITOLARE ED I RESPONSABILI ESTERNI DEL TRATTAMENTO

CAP. 3

❖ IL RESPONSABILE ESTERNO DEL TRATTAMENTO: RUOLO E GESTIONE DEI RAPPORTI

Il Responsabile del trattamento dati o "data processor", come definito in generale dall'art. 4 comma 1 n. 8 del GDPR n. 679/2016, è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento*".

L'art. 28, in particolare, dispone quanto segue: "*Qualora un trattamento debba essere effettuato per conto del Titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. Il responsabile del trattamento non ricorre ad altro responsabile senza previa autorizzazione scritta, specifica generale, del Titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il Titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al Titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare…*".

Il Responsabile del trattamento è un soggetto esterno alla struttura aziendale del Titolare, al quale quest'ultimo affida l'espletamento di servizi o prestazioni che comportano un trattamento di dati personali, le cui modalità sono disciplinate compiutamente in apposito contratto di nomina. Tale contratto stabilisce un rapporto che vincola il Responsabile al pieno rispetto delle istruzioni impartite dal Titolare, al quale spetta inoltre l'obbligo di vigilanza e verifica.

In conformità a quanto disposto dal citato art. 28 GDPR, il Responsabile deve offrire al Titolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti stabiliti dalla normativa europea e garantisca la tutela dei diritti dell'interessato.

I trattamenti da parte di ciascun Responsabile esterno del Titolare devono essere definiti da un atto giuridica redatto a norma del diritto dell'Unione o degli Stati membri, secondo lo schema contrattuale allegato alla presente procedura quale parte integrante e sostanziale, che lo vincoli all' Azienda, Titolare del trattamento, e che regolamenti la tipologia di dati trattati,la durata del trattamento, la natura e la finalità dello stesso, le categorie di interessati , nonché gli obblighi e i diritti del Titolare del trattamento.

In conformità a quanto stabilito all'art. 28, co. 3 del GDPR il contratto, vincolante, tra il Titolare del trattamento dei dati ed il Responsabile esterno del trattamento deve prevedere in particolare a carico di quest'ultimo i seguenti obblighi:

1. trattare i dati solo in conformità alle istruzioni ricevute dal Titolare, anche in ipotesi di trasferimento dei dati al di fuori dell'Unione Europea;
2. garantire che le persone fisiche autorizzate alle attività di trattamento siano vincolate da obblighi di riservatezza, contrattualmente assunti o stabiliti per legge;
3. adottare le misure richieste ai sensi dell'art. 32 del Regolamento Europeo, ovvero le misure tecniche e organizzative a protezione dei dati ritenute idonee a garantire un livello di sicurezza adeguato al rischio insito nel trattamento;
4. acquisire, in caso di ricorso al subappalto, preventiva autorizzazione scritta da parte del Titolare.

Altri doveri in capo al Responsabile esterno sono:

- rispondere direttamente nei confronti del Titolare per eventuali inadempimenti della propria catena di subfornitura;
- informare il Titolare, qualora abbia ricevuto un'autorizzazione generale al subappalto, di eventuali variazioni in ordine alla modifica o alla sostituzione di taluno dei propri subappaltatori, dando così l'opportunità al Titolare di opporsi a tali modifiche;
- assistere il Titolare fornendo supporto anche alle eventuali richieste degli interessati (accesso, rettifica, cancellazione, portabilità, opposizione);
- assicurare protezione ai dati attraverso misure tecniche e organizzative adeguate, ai sensi dell'art. 32 del GDPR;
- effettuare la valutazione d'impatto (impact assessment) richiesta dall'art. 35 del GDPR;
- consultare l'Autorità, qualora la valutazione d'impatto effettuata indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal Titolare del trattamento per attenuare il rischio;
- cancellare o restituire i dati, su scelta del Titolare, al momento della cessazione del rapporto, salvo che la legge non imponga specifici obblighi di conservazione;
- mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi di cui al presente elenco;
- consentire al Titolare di effettuare attività di audit, direttamente o per il tramite di terze parti all'uopo incaricate.

❖ PROCEDURA PER LA DESIGNAZIONE DEI RESPONSABILI DEL TRATTAMENTO

Qualora un trattamento venga affidato a persona fisica o giuridica esterna alla struttura del Titolare, che opera o presta un servizio in nome e per conto di esso, questa deve essere designata Responsabile del trattamento. Qualora il Titolare non ritenga necessario ricorrere a tale designazione, rimane unico responsabile nei confronti dell'Autorità di Controllo e nei confronti degli Interessati.

I trattamenti affidati a ciascun Responsabile devono essere disciplinati da un contratto o altro atto giuridico scritto, da cui si evinca in maniera chiara il rapporto di subordinazione del Responsabile al potere di indirizzamento e controllo esercitato dal Titolare, relativamente ad ogni circostanza riconducibile al/i trattamento/i affidato/i.

Negli accordi, nelle convenzioni e nei contratti di affidamento di attività o di servizi all'esterno dell'Azienda, la Struttura preposta alle fasi di contrattualizzazione del rapporto (es. UOC Acquisizione Beni e Servizi, UOC Affari Generali, UOC Ingegneria Clinica, UOC Sistemi Informatici etc.),deve sottoporre al Responsabile l'apposito contratto di nomina, con il quale il soggetto affidatario si impegna, per i trattamenti dei dati effettuati in forza del rapporto contrattuale, all'osservanza delle norme di legge sulla protezione dei dati personali e delle disposizioni dell'Azienda in materia.
La nomina si perfeziona con la sottoscrizione del relativo atto, contestualmente a quella del contratto/convenzione.
La struttura aziendale procedente ha l'obbligo di utilizzare lo schema di nomina predisposto dalla UOS Privacy e allegato al presente documento.
La struttura aziendale procedente dovrà trasmettere alla UOS Privacy, preliminarmente alla stipula del contratto con il fornitore di servizi, la bozza di atto di nomina, congiuntamente alla documentazione contrattuale relativa al rapporto di fornitura, al fine di consentire alla predetta UOS di valutare la correttezza formale e sostanziale della nomina a Responsabile esterno.

Tutti i Delegati al trattamento dei dati, individuati nei Direttori delle Strutture aziendali procedenti, in quanto responsabili dell'istruttoria finalizzata all'affidamento di attività, prestazioni o servizi, nonché il Direttore dell'UOC Affari Generali, in quanto responsabile dell'istruttoria per la stipula di convenzioni, d'intesa con la UOS Privacy, sono tenuti a fornire la propria collaborazione al fine di addivenire alla stesura delle nomine dei Responsabili Esterni del Trattamento.

In particolare, procederanno alle seguenti attività:
• Inserimento, nei Disciplinari di Gara, dell'Informativa sul trattamento dei dati (all. n.4);
• predisposizione, avvalendosi della consulenza della UOS Privacy, del Contratto di nomina a Responsabile esterno del Trattamento dei dati (all. n. 1).

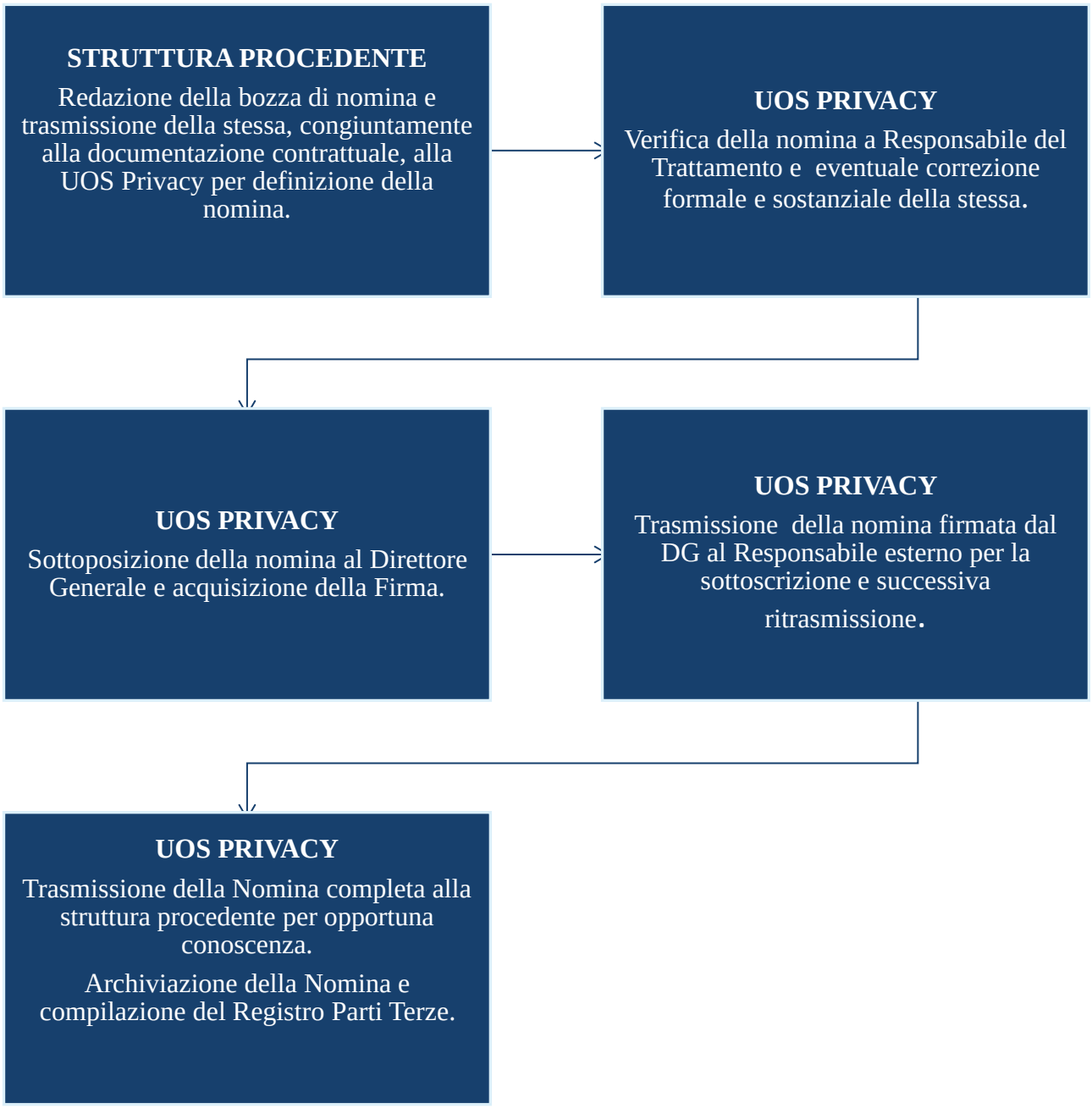
Nell'ambito della presente procedura, dopo aver definito il Contratto di nomina a Responsabile esterno del Trattamento, sarà cura della UOS Privacy provvedere a:

• sottoporre il Contratto alla firma del Direttore Generale;
• trasmettere il Contratto di nomina al Responsabile del Trattamento (persona fisica o giuridica), per l'acquisizione della firma per accettazione.

Predetta UOS, appena verrà ultimato il processo summenzionato, avrà inoltre cura di informare la Struttura procedente dell'avvenuta stipula e aggiornare il Registro Parti Terze dell'Azienda, contenente gli estremi identificativi dei Responsabili, nonché le informazioni relative ai servizi affidati.

Si rappresenta che, nel caso di Raggruppamenti Temporanei di Impresa costituiti per erogare servizi al Titolare, il ruolo di Responsabile può essere attribuito a ciascuna delle imprese costituenti il RTI, relativamente al proprio specifico ambito di fornitura. Nel caso di raggruppamenti permanenti, quali ad esempio consorzi stabili e società consortili, cooperative ed altre tipologie di associazioni che si configurano come soggetto giuridico, è preferibile la designazione di un unico Responsabile del trattamento.

WORKFLOW RIEPILOGATIVO DEL PROCESSO DI NOMINA DEL RESPONSABILE ESTERNO



❖ REVISIONE DEI CONTRATTI IN ESSERE

Per i contratti e le convenzioni stipulati in data antecedente alla presente procedura, le Strutture procedenti dovranno effettuare la ricognizione di quelli già in essere tra il Titolare e soggetti esterni (persone fisiche o giuridiche) aventi ad oggetto attività, prestazioni o servizi che comportano operazioni di trattamento e/o elaborazione dei dati personali. Tanto al fine di procedere all'aggiornamento, integrazione o regolarizzazione di tutti i rapporti giuridici esistenti, in applicazione del Regolamento.

Effettuata la predetta ricognizione, le Strutture a cui afferiscono i contratti di fornitura di beni e servizi dovranno:

• dare comunicazione alla UOS Privacy tramite la casella mail uosprivacy@aslnapoli3sud.it dell'avvenuta stipula del Contratto di nomina a responsabile esterno del trattamento, utilizzando il modello allegato **(all. n.3).**

• inviare tempestivamente l'elenco di tali contratti di nomina alla UOS Privacy all'indirizzo uosprivacy@aslnapoli3sud.it.

Si rappresenta l'assoluta necessità di mettere a sistema quanto regolamentato, al fine di evitare situazioni non correttamente censite delle quali si farà comunque carico il competente Delegato interno al trattamento dei dati personali.

Pertanto, laddove le strutture aziendali non abbiamo provveduto a stipulare i contratti di nomina per alcuni rapporti in essere, sono tenute ad attivare la summenzionata procedura, al fine di consentire una piena regolamentazione dei rapporti privacy e la corretta tenuta del Registro Parti Terze, a cura della UOS Privacy.

❖ CANALI DI COMUNICAZIONE

I Dirigenti preposti alle attività che prevedono un trattamento di dati personali esternalizzato, avranno cura di gestire le comunicazioni con i Responsabili, avvalendosi del supporto della UOS Privacy e della consulenza del DPO Aziendale.

Si segnala che le comunicazioni con i Responsabili in merito alle tematiche di seguito elencate, dovranno avvenire a mezzo PEC.

- Richieste da parte degli Interessati effettuate nell'esercizio dei propri diritti di cui al capo III del Regolamento.
- Constatazione di violazioni di sicurezza riconducibili all'operato del Responsabile (data breach).
- Pronunciamenti, rilievi e sanzioni stabiliti dall'Autorità di Controllo (Garante della protezione dei dati personali), riguardanti i trattamenti e/o i dati personali riconducibili al Responsabile.
- Copia del Registro dei trattamenti redatto e aggiornato dal Responsabile, relativamente alle sole parti riconducibili ai trattamenti oggetto del contratto.
- Copia della documentazione e successivi aggiornamenti relativi alle valutazioni di impatto e di rischio svolte dal Responsabile, riconducibili ai trattamenti oggetto del contratto.

- Proposte di designazione di sub-responsabili, formulate dal Responsabile e sottoposte ad approvazione del Titolare.
- Richieste di variazione sulle informative e sulle eventuali modalità di acquisizione dei consensi da parte degli Interessati del trattamento di dati personali riconducibili ai trattamenti oggetto del contratto;
- Ogni altra tipologia di comunicazione che si ritenga rilevante, ai fini della corretta gestione dei trattamenti e dei dati personali riconducibili all'oggetto del contratto.

Tutte le comunicazioni relative al trasferimento di informazioni personali devono essere effettuate adottando le misure di protezione indicate dal Titolare.

❖ EVENTUALE DESIGNAZIONE DI SUB-RESPONSABILI

Il Sub-responsabile è una figura introdotta dal GDPR per definire un soggetto che opera in virtù di un contratto stipulato con il Responsabile del trattamento, che lo vincola al pieno rispetto delle istruzioni impartite dallo stesso.

Un Responsabile designato dal Titolare non può designare altri Responsabili (sub-responsabili) che lo supportino nel trattamento dei dati personali a lui affidato, senza un'autorizzazione scritta da parte del Titolare **(all. n.2)**.

Il Responsabile ha dunque l'obbligo di comunicare preventivamente questa intenzione al Titolare, che ha la facoltà di opporsi (art.28 par. 2 del Regolamento). In particolare, nei casi in cui l'impresa che tratta dati personali per conto del Titolare, sia intenzionata a subappaltare parte di tali attività, questa ha l'obbligo di comunicare al Titolare del trattamento la propria intenzione di designare uno o più sub-responsabili, individuati tra le imprese subappaltatrici.

Nei casi in cui il Titolare ricorra a procedure di gara per l'acquisizione di forniture di beni e servizi o prestazioni professionali, è opportuno esplicitare nel capitolato di gara:

- l'impegno da parte della società appaltatrice ad accettare il ruolo di Responsabile mediante contratto/atto giuridico, seguito dalle istruzioni impartite dal Titolare, compreso l'impegno ad impartire istruzioni e vigilare sull'operato degli eventuali sub-responsabili;
- l'autorizzazione generale a designare sub-responsabili del trattamento concessa in via preliminare dalla stazione appaltante (Committente e Titolare del trattamento) alla società appaltatrice (futura Responsabile del trattamento), fermo l'obbligo di comunicare preventivamente il nome del sub-responsabile. Nel caso in cui il Responsabile faccia effettivo ricorso a sub-responsabili, egli si impegna a selezionare sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti in merito a trattamenti effettuati in applicazione della normativa pro tempore vigente e che garantiscano la tutela dei diritti degli interessati. Il Responsabile si impegna, altresì, a stipulare specifici contratti, o altri atti giuridici, con i sub-responsabili a mezzo dei quali il Responsabile descriva analiticamente i loro compiti e imponga a tali soggetti di rispettare i medesimi obblighi, con particolare riferimento alla disciplina sulla protezione dei dati personali.

L'autorizzazione o il diniego da parte del Titolare alla designazione di sub-responsabili è indipendente da ogni altra autorizzazione al subappalto afferente alla commessa, ovvero l'autorizzazione al subappalto non costituisce implicita autorizzazione a designare sub-responsabili del trattamento.

Qualora il sub-responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dei sub-responsabili coinvolti. Il Responsabile informa il Titolare di eventuali modifiche previste riguardanti

l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

Le clausole contrattuali che regolamentano la designazione del sub-responsabile da parte del Responsabile seguono, applicando le dovute contestualizzazioni, le medesime indicazioni valide per la designazione del Responsabile.

CAPITOLO 4
GESTIONE DEI DATI PERSONALI OGGETTO DI TRATTAMENTO

CAP. 4

❖ INDIVIDUAZIONE DEI TRATTAMENTI E DEI DATI PERSONALI AFFIDATI AI RESPONSABILI

L'art. 30 del Regolamento stabilisce l'obbligo di redigere ed aggiornare nel tempo un "Registro delle attività di trattamento", estendendo tale obbligo anche al Responsabile, relativamente ai trattamenti svolti per conto del Titolare del trattamento (art.30 par.2).

Il Titolare ha l'obbligo di indicare i riferimenti del Responsabile nel proprio registro dei trattamenti e a sua volta il Responsabile ha l'obbligo di indicare i riferimenti del Titolare del trattamento nel proprio Registro. Il Titolare del trattamento può altresì fornire indicazioni vincolanti circa le modalità di compilazione e aggiornamento delle registrazioni dei trattamenti svolti dal Responsabile per suo conto.

L'art. 35 del Regolamento introduce l'obbligo di svolgere le valutazioni di impatto sulla protezione dei dati (DPIA) per alcune tipologie di trattamento dati sottoposti a rischi rilevanti di violazioni della sicurezza.

Nel caso di trattamenti svolti da un Responsabile, il Titolare si riserva di chiedere al soggetto esterno copia della DPIA effettuata, al fine di verificare l'esito della valutazione d'impatto e i possibili rischi.

❖ GESTIONE DELLE INFORMATIVE AGLI INTERESSATI

Qualora il Responsabile, nello svolgimento dei trattamenti a lui affidati, abbia la necessità di raccogliere dati personali direttamente presso gli Interessati, è obbligato ad informare gli interessati al momento della raccolta dei dati, secondo quanto disposto nell'art. 13 del Regolamento.

Per adempiere a tale obbligo, il Responsabile sottopone all'approvazione del Titolare una bozza del documento di "Informativa all'Interessato" ex art.13 GDPR, con l'obbligo di recepire tutte le eventuali modifiche richieste dal Titolare.

❖ GESTIONE DEGLI ADEMPIMENTI PER L'ESERCIZIO DEI DIRITTI DELL'INTERESSATO

L'esercizio dei diritti dell'interessato di cui agli artt. da 15 a 22 del Regolamento, qualora riguardi in tutto o in parte i trattamenti affidati al Responsabile, richiede la collaborazione attiva del Responsabile il quale dovrà estendere tale obbligo di collaborazione anche agli eventuali sub-responsabili designati.

Nell'ambito delle istruzioni che il Titolare fornisce ai Responsabili, sono da ritenersi come adempimento contrattuale obbligatorio, l'osservanza scrupolosa delle disposizioni impartite mediante il seguente documento, avente carattere di indirizzamento e regolamentazione:

- "Procedura per la gestione dei diritti degli interessati", che stabilisce ruoli, responsabilità e modalità operative per la gestione dei diritti dell'Interessato presso il Titolare, in tutti i casi previsti dal Regolamento.

L'aderenza alla suddetta procedura si intende obbligatoriamente applicabile anche nei casi in cui le richieste dell'Interessato siano indirizzate solo al Responsabile e/o riguardino esclusivamente trattamenti a lui affidati.

❖ GESTIONE DELLE VIOLAZIONI DELLA SICUREZZA DEI DATI PERSONALI

Qualora il Responsabile rilevi violazioni o sospette violazioni della sicurezza dei dati personali trattati per conto del Titolare, egli è tenuto, a seguire scrupolosamente le disposizioni impartite dal Titolare, ed in particolare quelle documentate nella "Procedura per la gestione del data breach".

❖ GESTIONE DELLE VERIFICHE SVOLTE DAL TITOLARE

Al momento della designazione, il Responsabile assume l'impegno contrattuale ad acconsentire ed agevolare le verifiche effettuate dal Titolare del trattamento, dal DPO e/o da terze parti incaricate. Questo impegno è inoltre stabilito dall'art. 28, lettera h del Regolamento, che obbliga il Responsabile a "*mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato*".

❖ DISPOSIZIONI FINALI

Ciascun Delegato del Titolare, per quanto di competenza, avrà cura di impartire precise disposizioni al personale dipendente in modo da assicurare il rispetto della presente procedura e la sua corretta applicazione.

Il Responsabile della protezione dei dati (DPO) fornisce il proprio supporto per eventuali dubbi, chiarimenti ed approfondimenti.

La presente procedura è suscettibile di eventuali modifiche, aggiornamenti ed integrazioni, nel caso le stesse si rendessero necessarie o opportune.

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
TEL 081/8490645- PROTOCOLLO@PEC.ASLNAPOLI3SUD.IT

CAPITOLO 6
ALLEGATI

❖ DOCUMENTI ALLEGATI

Allegato n. 1	**Contratto di nomina a Responsabile Esterno**
Allegato n. 2	**Autorizzazione alla nomina di sub-Responsabili**
Allegato n.3	**Modello di comunicazione della nomina a Responsabile esterno alla UOS Privacy**
Allegato n.4	**Informativa sul trattamento dei dati personali dei Fornitori ex art.13 GDPR**