



N. 18/2023/Reg.Decr.

Montelupo Fiorentino lì, 06/03/2023

OGGETTO: NOMINA RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI DEL SERVIZIO GESTIONE RISORSE

IL SINDACO

Premesso che

- l'art. 2 *quaterdecies* ("Attribuzione di funzioni e compiti a soggetti designati") del Codice in materia di protezione dei dati personali (D.Lgs. n. 196/2003), integrato con le modifiche introdotte dal D.Lgs. n. 101/2018, stabilisce che *"Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta"*;
- nell'ambito delle attività svolte dal Titolare è sorta l'esigenza di avvalersi di uno o più Responsabile interno/Designato del trattamento dei dati personali (di seguito, per brevità anche "Responsabile interno") per lo svolgimento di attività specifiche di seguito indicate;
- è necessario delegare ai responsabili di servizio designati, l'esercizio e lo svolgimento degli specifici compiti e funzioni attribuite;
- il soggetto designato è disposto ad assolvere l'incarico di Responsabile interno e ha la competenza per svolgerlo;

- i responsabili di servizio, sono responsabili, in via esclusiva, dell'attività amministrativa, della gestione e dei risultati della struttura organizzativa a cui sono preposti;
- la nomina di Responsabile interno e la relativa autorizzazione al trattamento dei dati permane efficace sino al perdurare del rapporto di natura lavorativa con il Titolare, salvo diversa previsione da parte del Titolare, e potrà essere revocata in qualsiasi momento dallo stesso;
- al Responsabile interno è concessa la facoltà di nominare un "altro Responsabile interno" (c.d. "Sub Responsabile interno") con riferimento al settore di propria spettanza;
- è concessa inoltre la facoltà al Responsabile interno di nominare Responsabili esterni del trattamento dei dati personali, ai sensi dell'art. 28, par. 1, del GDPR,

DECRETA

di designare Migliori Maria Teresa, Responsabile del Servizio Gestione Risorse, nominata con decreto del Sindaco n. 36 del 27/05/2022; ad operare sotto la diretta autorità del Titolare, quale Responsabile interno del trattamento persona fisica a cui attribuire specifici compiti e funzioni connessi al trattamento di dati personali, relativi ai trattamenti rientranti nella struttura organizzativa di competenza, e di seguito elencati, e nominare lo stesso quale Responsabile interno del trattamento dei dati personali, delegando tutti i compiti in relazione alla eventuale nomina degli Amministratori di sistema e degli Incaricati/Autorizzati del trattamento, i seguenti responsabili di servizio.

AUTORIZZA PER QUANTO ATTIENE AD "ALTRI RESPONSABILI"

il suddetto Responsabile interno a nominare a sua volta "Altri Responsabili del Trattamento" (Sub Responsabili interni o Responsabili esterni).

Agli "Altri Responsabili del Trattamento" si applicano tutti gli obblighi di seguito indicati che devono essere formalizzati mediante uno specifico atto.

Gli "Altri Responsabili del Trattamento" devono offrire garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti normativi e garantisca la tutela dei diritti dell'interessato,

AUTORIZZA

con decorrenza dalla data di sottoscrizione del presente atto, il Responsabile interno a trattare dati personali, conformemente al G.D.P.R., alla normativa interna di adeguamento, alle Linee guida delle Autorità di controllo, e alle specifiche istruzioni indicate dal Titolare sulle modalità a cui attenersi nel trattamento,

Trattamenti affidati al Responsabile del trattamento

Il Titolare affida al Responsabile il trattamento di tutti i dati personali relativamente alle attività afferenti al settore di sua competenza. In particolare: tutti i trattamenti necessari allo svolgimento dei processi, compiti e funzioni di competenza del settore al quale il medesimo è preposto, in base all'organizzazione interna del Titolare o in base a specifici atti di assegnazione, inclusi i trattamenti che possono presentare rischi elevati ai sensi dell'articolo 35 del GDPR.

Operazioni trattamento eseguibili: tutte le operazioni di trattamento dei dati personali, nessuna esclusa che si rendono necessarie per la gestione dei processi/procedimenti/attività, compiti e funzioni di competenza dell'unità organizzativa medesima, incluse tutte le operazioni di trattamento relative ai trattamenti che possono presentare rischi elevati ai sensi dell'articolo 35 del GDP.

Archivi/Banche dati: tutti gli archivi e le banche dati, nessuna esclusa che si rendono necessarie per la gestione dei processi/procedimenti/attività, compiti e funzioni di competenza dell'unità organizzativa medesima, incluse le operazioni di trattamento relative ai trattamenti che possono presentare rischi elevati ai sensi dell'articolo 35 del GDPR.

Durata del trattamento

Il trattamento avrà durata pari alla durata del rapporto tra le parti. All'esaurirsi del rapporto, il Responsabile non sarà più autorizzato ad eseguire i trattamenti per conto del Titolare.

Doveri e compiti del Responsabile del trattamento

Con la sottoscrizione della presente nomina il Responsabile si impegna a garantire la correttezza del trattamento, nonché adeguate misure di sicurezza a protezione dei dati trattati.

Nello specifico il Responsabile interno dovrà:

- trasferire i dati personali verso un Paese terzo extra UE soltanto previa istruzione documentata del Titolare del trattamento. Laddove il trasferimento sia richiesto dal diritto dell'Unione Europea o dalla normativa nazionale cui è soggetto il Titolare, il Responsabile dovrà informare il Titolare circa tale obbligo giuridico prima del trattamento;
- garantire che le persone Incaricate/autorizzate al trattamento dei dati personali siano state nominate con provvedimento e che le stesse si siano impegnate a rispettare gli obblighi di segretezza e riservatezza, anche per il periodo successivo all'estinzione del rapporto lavorativo intrattenuto con il Titolare del trattamento, in relazione alle operazioni di trattamento da esse eseguite;
- impartire per iscritto, agli Incaricati al trattamento, istruzioni in merito alle operazioni di trattamento dei dati personali e a vigilare sulla loro puntuale applicazione;
- adottare tutte le misure di sicurezza previste dalla normativa ed in particolare, ove applicabili, le misure previste dall'art. 32 del Regolamento;
- adottare misure tecniche e organizzative adeguate a proteggere i dati personali e nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 "Sicurezza del Trattamento", tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento;
- mettere a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Regolamento;

Tipologia di dati personali oggetto del trattamento e categorie di interessati

Tutte le categorie di dati personali, anche le particolari categorie di dati di cui agli artt. 9 e 10 GDPR, che si rendono necessarie allo svolgimento dei compiti e delle funzioni di competenza del designato, inclusi gli archivi e le banche dati relativi ai trattamenti che possono presentare rischi elevati ai sensi dell'articolo 35 del GDPR.

Obblighi e diritti del Responsabile del trattamento

Il Responsabile deve tenere aggiornato l'elenco degli estremi identificativi delle persone fisiche preposte quali Incaricati del trattamento e Amministratore di Sistema.

Il Responsabile si impegna ad informare tempestivamente gli "Altri Responsabili del trattamento", fornendo istruzioni documentate, in caso di variazioni o cambiamenti nelle operazioni di trattamento dei dati. Il Responsabile dovrà vigilare sull'operato degli "Altri Responsabili del trattamento" mediante esecuzione di controlli specifici eseguibili ad opera

del Responsabile stesso o attraverso la collaborazione di altro soggetto specificamente incaricato.

ELENCO DEGLI SPECIFICI COMPITI E FUNZIONI ATTRIBUITI AL RESPONSABILE DI SERVIZIO E CONNESSI AL TRATTAMENTO DEI DATI PERSONALI

- collaborare con gli altri responsabili di servizio, designati e delegati, per l'elaborazione degli obiettivi strategici e operativi del sistema di sicurezza e di protezione dei dati personali, sensibili e giudiziari, da sottoporre all'approvazione del titolare;
- collaborare con gli altri responsabili di servizio, designati e delegati, per l'elaborazione della pianificazione strategica del sistema di sicurezza e di protezione dei dati personali, sensibili e giudiziari attraverso l'elaborazione di un Piano per la sicurezza/protezione, da sottoporre all'approvazione del titolare;
- collaborare con il titolare del trattamento per inserimento degli obiettivi strategici e operativi del sistema di sicurezza e di protezione dei dati personali nel Piano della Performance/PDO nonché nel DUP e negli altri strumenti di pianificazione del titolare;
- identificare contitolari, responsabili e sub responsabili di riferimento della struttura organizzativa di competenza, e sottoscrivere gli accordi interni e i contratti per il trattamento dei dati, avendo cura di tenere costantemente aggiornati i documenti relativi ai contitolari e ai responsabili;
- di acquisire dai contitolari, responsabili e sub responsabili l'elenco nominativo delle persone fisiche che, presso gli stessi contitolari, responsabili e sub responsabili risultano autorizzate al trattamento dei dati e a compiere le relative operazioni;
- identificare e designare, per iscritto e in numero sufficiente a garantire la corretta gestione del trattamento dei dati inerenti la struttura organizzativa di competenza, le persone fisiche della struttura organizzativa medesima, che operano sotto la diretta autorità del titolare, e attribuire alle persone medesime specifici compiti e funzioni inerenti al trattamento dei dati, conferendo apposita delega per l'esercizio e lo svolgimento degli stessi, inclusa l'autorizzazione al trattamento, impartendo a tale fine analitiche istruzioni, e controllando costantemente che le persone fisiche designate, delegate e autorizzate al trattamento dei dati effettuino le operazioni di trattamento:

- in attuazione del principio di "liceità, correttezza e trasparenza";
 - in attuazione del principio di "minimizzazione dei dati";
 - in attuazione del principio di "limitazione della finalità";
 - in attuazione del principio di "esattezza";
 - in attuazione del principio di "limitazione della conservazione";
 - in attuazione del principio di "integrità e riservatezza";
 - in attuazione del principio di "liceità, correttezza e trasparenza".
- effettuare la ricognizione integrale di tutti i trattamenti di dati personali, sensibili e giudiziari svolti nella struttura organizzativa di competenza, in correlazione con i processi/ procedimenti svolti dall'Ufficio, da sottoporre all'approvazione del titolare;
 - effettuare l'aggiornamento periodico, almeno annuale e, comunque, in occasione di modifiche normative, organizzative, gestionali che impattano sui trattamenti, della ricognizione dei trattamenti al fine di garantirne la costante rispondenza alle attività effettivamente svolte dalla struttura organizzativa, con obbligo di sottoporre l'aggiornamento all'approvazione del titolare;
 - effettuare l'analisi del rischio dei trattamenti, e la determinazione preliminare dei trattamenti che possono presentare un rischio elevato per i diritti e le libertà degli interessati, da sottoporre all'approvazione del titolare;
 - effettuare prima di procedere al trattamento, quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, una valutazione dell'impatto del trattamento sulla protezione dei dati personali;
 - mettere in atto le misure tecniche e organizzative adeguate, identificate dal titolare, funzionali a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
 - a) la pseudonimizzazione e la cifratura dei dati personali;
 - b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

- mettere in atto le misure tecniche e organizzative adeguate identificate dal titolare per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, fermo restando che:
 - a) tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità;
 - b) dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica
- proporre e suggerire al titolare misure tecniche e organizzative ritenute necessarie garantire la protezione dei dati dal trattamento, in relazione ai trattamenti della struttura organizzativa di competenza;
- tenere il registro delle attività di trattamento in relazione ai trattamenti della struttura organizzativa di competenza;
- cooperare, su richiesta, con il RPD/PDO e con l'Autorità di controllo nell'esecuzione dei suoi compiti;
- in caso di violazione dei dati personali, collaborare con il titolare, il RPD/PDO per notificare la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche;
- in caso di violazione dei dati personali, comunicare la violazione all'interessato senza ingiustificato ritardo, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche,
- prima di procedere al trattamento, consultare l'Autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio;
- assicurarsi che il RPD/PDO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali;
- sostenere il RPD/PDO nell'esecuzione dei compiti fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica;

- documentare e tracciare, per iscritto, ed essere in grado di provare, in caso di richiesta dell'Autorità di controllo, l'attuazione del sistema di sicurezza finalizzato alla protezione dei dati personali;
- collaborare con il titolare per inserimento dei rischi di corruzione, illegalità e degli illeciti in materia di trattamento di dati personali negli aggiornamenti annuali al PTPC e collaborare al RPC per le segnalazioni degli illeciti relativi al trattamento dei dati;
- collaborare con gli altri responsabili di servizio designati e delegati e con il Segretario per l'elaborazione e l'aggiornamento delle procedure necessarie al sistema di sicurezza e, in particolare per la procedura da utilizzare in caso di data breach, da sottoporre all'approvazione del titolare;
- documentare tutte le attività e adempimenti delegati e, in ogni caso, tracciare documentalmente l'intero processo di gestione dei rischi e del sistema di sicurezza e protezione;
- controllare e monitorare la conformità dell'analisi, della valutazione dei rischi, e dalla valutazione di impatto nonché e controllare e monitorare la conformità del trattamento dei rischi al contesto normativo, regolamentare, regolatorio, gestionale, operativo e procedurale, con obbligo di tempestiva revisione in caso di rilevazioni di non conformità o di scostamenti;
- tracciare documentalmente le attività di controllo e monitoraggio mediante periodici report/resoconti/referti da sottoporre al titolare e al RPD/PDO;
- conformare il trattamento ai pareri e indicazioni del RPD/PDO e dell'Autorità di controllo nonché alle linee guida e ai provvedimenti dell'Autorità di controllo;
- formulare proposte, in occasione dell'approvazione/aggiornamento annuale degli strumenti di pianificazione e programmazione, volte ad implementare il sistema di sicurezza e ad elevare il livello di protezione degli interessati;
- attuare la formazione in tema di diritti e libertà degli interessati, di rischi di violazione dei dati, di informatica giuridica, e di diritto
- promuovere la cultura della prevenzione del rischio di violazione dei dati e la cultura della protezione come valore da integrare in ogni processo/procedimento;
- effettuare ogni ulteriore attività, non espressamente indicata in precedenza e necessaria per la integrale attuazione del GDPR e della normativa interna di adeguamento.

Per quanto non previsto e non riportato sul presente atto di nomina si rinvia alla normativa vigente in materia di protezione e sicurezza dei dati personali, nonché alla normativa nazionale prevista in materia (in particolare: al Regolamento UE 2016/679 e al Codice in materia di protezione dei dati personali, D.Lgs. n. 196/2003, integrato con le modifiche del D.Lgs. n. 101/2018).

Il Sindaco

MASETTI PAOLO / ArubaPEC S.p.A.