

Rep. N. _____

Disciplinare di incarico di Responsabile Protezione Dati (RPD) / Data Protection Officer (DPO) e di Responsabile del Trattamento dei dati

L'anno duemilaventuno, il giorno _____ del mese di _____, presso la sede del CEFPAS di Caltanissetta sono presenti:

- l'Ing. Roberto Sanfilippo, nato a Genova il 4 aprile 1970, n.q. di Direttore e legale rappresentante del Centro, partita IVA 01427360852 e Titolare del trattamento dei dati
- il dott. _____, nato a _____ il _____, residente in _____, P.IVA _____.

PREMESSO

- con deliberazione _____ è stata disposta la sottoscrizione del contratto in favore della dott.ssa _____ per lo svolgimento del servizio di protezione dei dati (R.P.D.) /data protection officer (DPO) e responsabile del trattamento dati, per la durata di anni due;

Tutto ciò premesso,

l'Ing. Roberto Sanfilippo, n.q. di Direttore e legale rappresentante del Centro e Titolare del trattamento dei dati - in esecuzione della normativa vigente in materia di Protezione dei dati ed in particolare del Decreto Legislativo 196/2003, integrato con le modifiche introdotte dal D.lgs 101/2018, degli artt. 24 e seguenti del Regolamento generale sulla protezione dei dati, anche noto come GDPR (General Data Protection Regulation) approvato con Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016

NOMINA

L'avv. _____, nato a _____ il _____, residente in _____, P.IVA _____, Responsabile Protezione Dati (RPD) / Data Protection Officer (DPO) e Responsabile del Trattamento dei dati del CEFPAS (d'ora innanzi per brevità professionista), con strumenti elettronici o comunque automatizzati o con strumenti diversi, per l'ambito di attribuzioni, competenze e funzioni assegnate sia per le attività coerenti con i fini istituzionali sia per quelle del progetto "Sanità digitale della Regione Siciliana" - SPC CLOUD LOTTO1.

Art.1 - OGGETTO DELL'INCARICO

Il RPD/DPO svolge un ruolo chiave nel promuovere la cultura della protezione dati all'interno dell'Azienda e contribuisce a dare attuazione ad elementi essenziali del Regolamento Europeo per il trattamento dei dati personale (Reg. UE 2016/679) quali:

- i principi fondamentali del trattamento;
- i diritti degli interessati;
- la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita;
- i registri delle attività di trattamento;
- la sicurezza dei trattamenti;
- la notifica e comunicazione delle violazioni dei dati personali.

CATEGORIE DEGLI INTERESSATI E NATURA E FINALITÀ DEL TRATTAMENTO

Il trattamento avrà ad oggetto le seguenti categorie di interessati:

- personale dipendente del CESPAS;
- persone fisiche che usufruiscono dei servizi che il CEFPAS offre all'esterno (corsi didattici, esami);
- terzi che entrano in contatto col CEFPAS in dipendenza della sua attività istituzionale.

Saranno trattati dati personali, non sanitari e non biometrici. Quanto alla prima categoria, anche i dati relativi agli accessi e alle uscite ed in generale quelli normalmente necessari alla gestione dei rapporti di lavoro del personale dipendente.

Al dott. _____ sono affidate le funzioni disciplinate dal Regolamento UE2016/79 e precisamente:

- informare e fornire consulenza al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente Regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del presente Regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità,
- sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo e, in particolare, a quello in servizio presso il servizio SIA;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Reg. UE 2016/679;
- cooperare con l'Autorità di Controllo;

- cooperare con il Responsabile per la prevenzione della corruzione e della trasparenza, per l'adeguamento e l'aggiornamento del Piano Triennale della prevenzione della corruzione e della trasparenza e del portale Trasparenza;
- fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Reg. UE 2016/679 ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;
- predisporre e gestire il Registro dei trattamenti;
- controllare che le violazioni dei dati personali siano documentate, notificate e comunicate;
- svolgere le funzioni comunque assegnate dalla normativa nel tempo vigente.
- garantire che il trattamento dei dati personali di cui è Titolare il CEFPAS e di cui venga a conoscenza con l'attività svolta avvenga in conformità a quanto previsto dalla vigente normativa e dalle presenti istruzioni ed in particolare nel rispetto dei principi di liceità, correttezza e trasparenza;
- aggiornare periodicamente l'elenco dei trattamenti dei dati personali e le relative banche dati gestite dal Centro; a tal fine, tenere un registro, come previsto dall'art. 30 del GDPR, in formato elettronico di tutte le categorie di attività relative al trattamento svolte per conto del Centro;
- mettere in atto, ai sensi dell'art. 32 del GDPR, tutte le misure tecniche ed organizzative necessarie a garantire un livello di sicurezza adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento effettuato;
- provvedere affinché vengano rigorosamente adottate tutte le misure idonee a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, gli accessi non autorizzati o trattamenti non consentiti o non conformi alle finalità per le quali i dati sono stati raccolti;
- verificare periodicamente lo stato di applicazione del D.lgs. 30 giugno 2003 n. 196 e del Regolamento Europeo 2016/679, nonché la corretta applicazione, il buon funzionamento dei sistemi e, ai sensi dell'art.32 del GDPR, delle misure adottate per la tutela dei dati personali e la conformità alle indicazioni dell'Autorità Garante e del Titolare del Trattamento;
- garantire la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali di titolarità del CEFPAS non coerente con l'incarico;
- garantire la portabilità dei dati personali trattati in esecuzione dell'incarico, ai sensi dell'art.20 del GDPR, assicurando che gli stessi possano essere trasmessi in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo automatico;
- assistere il Titolare del Trattamento per quanto concerne gli obblighi di notifica e ogni altra comunicazione verso il Garante, ove dovute;
- tenendo conto della natura del trattamento, assistere il Titolare del Trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del

Trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento Europeo 2016/679 e all'art.7 del D.lgs.196/2003;

- mettere a disposizione del Titolare del Trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente;
- comunicare al titolare del Trattamento qualsiasi variazione della situazione oggettiva o delle sue proprie caratteristiche soggettive, tali da compromettere il corretto espletamento dei compiti descritti nella presente;
- informare il Titolare del Trattamento senza ingiustificato ritardo e comunque non oltre le 72 ore dal momento in cui ne è venuto a conoscenza (art.33 del GDPR), di eventuali violazioni dei dati personali (Data breach) adottando, di concerto con lo stesso, nuove misure di sicurezza atte a circoscrivere gli effetti negativi dell'evento e a ripristinare la situazione precedente;
- predisporre e aggiornare un registro che dettagli, in caso di eventuali data breach, la natura delle violazioni, gli interessati coinvolti, le possibili conseguenze e le nuove misure di sicurezza implementate;
- supportare il Titolare del Trattamento durante la stesura della valutazione dell'impatto (ove prevista) dei trattamenti sulla protezione dei dati personali, nei casi in cui un tipo di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- supportare il Titolare del Trattamento durante le fasi di consultazione con l'autorità di controllo, qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento possa presentare un rischio elevato in assenza di misure adottate dal Titolare del Trattamento per attenuare il rischio;
- ottemperare tempestivamente alle eventuali richieste inoltrate dal Titolare del Trattamento al fine di rendere conforme il trattamento dei dati posto in essere agli eventuali provvedimenti emessi dal Garante Privacy in materia di trattamento dei dati personali;
- avvertire prontamente il CEFPAS, entro tre giorni lavorativi, in merito alle eventuali richieste degli interessati che dovessero pervenire al Responsabile e collaborare al fine di garantire il pieno esercizio da parte degli interessati di tutti i diritti previsti dall'articolo 7 del Codice;
- avvisare immediatamente, e comunque entro tre giorni lavorativi, il Titolare del Trattamento di qualsiasi richiesta o comunicazione da parte dell'Autorità Garante o di quella Giudiziarla o di Pubblica Sicurezza eventualmente ricevuta, inviando copia delle istanze per concordare congiuntamente il riscontro;
- verificare che i dati siano raccolti solo per finalità determinate, esplicite e legittime;
- costante informazione alla Direzione del Centro in merito a tutto ciò che concerne la protezione dei dati ed, in particolare, gli obblighi e gli adempimenti del datore di lavoro in materia.

Nell'eseguire i propri compiti il Responsabile della Protezione dei Dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Il Responsabile della Protezione Dati (RPD/DPO), è individuato anche come "Responsabile del Trattamento dei Dati", effettuato presso il CEFPAS, con strumenti elettronici o comunque automatizzati o con strumenti diversi, per conto del Titolare.

L'attività di Responsabile del trattamento dati è svolta in concomitanza all'esecuzione dell'incarico di RPD/DPO affidato, fino allo scadere dello stesso e, pertanto, nessun ulteriore compenso verrà corrisposto al medesimo incaricato.

Il Responsabile del trattamento dei dati ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni vigenti in materia e di osservare scrupolosamente quanto in essa previsto, nonché le seguenti istruzioni impartite dal Titolare. Il Responsabile del Trattamento si impegna ad impartire per iscritto, ai collaboratori autorizzati al trattamento, istruzioni in merito alle operazioni di trattamento dei dati personali ed a vigilare sulla loro puntuale applicazione.

COMPITI ED ISTRUZIONI PER IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI in applicazione del considerando art. 28 del Regolamento UE 2016/679.

PRINCIPI GENERALI DA OSSERVARE

Ogni trattamento di dati personali deve avvenire, nel rispetto primario dei seguenti principi di ordine generale:

per ciascun trattamento di propria competenza, il Responsabile deve fare in modo che siano sempre rispettati i seguenti presupposti:

- i dati devono essere trattati:
 - secondo il principio di liceità, vale a dire conformemente alle disposizioni del Regolamento, nonché alle disposizioni del Codice Civile, per cui, più in particolare, il trattamento non deve essere contrario a norme imperative, all'ordine pubblico ed al buon costume;
 - secondo il principio fondamentale di correttezza, il quale deve ispirare chiunque tratti qualcosa che appartiene alla sfera altrui;
- i dati devono essere raccolti solo per scopi:
 - determinati, vale a dire che non è consentita la raccolta come attività fine a se stessa;
 - espliciti, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
 - legittimi, cioè, oltre al trattamento, come è evidente, anche il fine della raccolta dei dati deve essere lecito;

- compatibili con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione e diffusione degli stessi;
- i dati devono, inoltre, essere:
 - esatti, cioè, precisi e rispondenti al vero e, se necessario, aggiornati;
 - pertinenti, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, in relazione all'attività che viene svolta;
 - completi: non nel senso di raccogliere il maggior numero di informazioni possibili, bensì di contemplare specificamente il concreto interesse e diritto del soggetto interessato;
 - non eccedenti in senso quantitativo rispetto allo scopo perseguito, ovvero devono essere raccolti solo i dati che siano al contempo strettamente necessari e sufficienti in relazione al fine, cioè la cui mancanza risulti di ostacolo al raggiungimento dello scopo stesso;
 - conservati per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle disposizioni aventi ad oggetto le modalità ed i tempi di conservazione degli atti amministrativi. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione e diffusione non è più consentita.

In particolare, i dati idonei a rivelare lo stato di salute o la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'interessato al trattamento, ovvero deve essere effettuato eliminando ogni occasione di impropria conoscibilità dei dati da parte di terzi.

Se il trattamento di dati è effettuato in violazione dei principi summenzionati e di quanto disposto dal Regolamento è necessario provvedere al "blocco" dei dati stessi, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del medesimo trattamento (ad esempio fornendo l'informativa omessa), ovvero alla cancellazione dei dati se non è possibile regolarizzare.

COMPITI PARTICOLARI DEL RESPONSABILE

Il Responsabile del trattamento dei dati personali, operando nell'ambito dei principi sopra ricordati, deve attenersi ai seguenti compiti di carattere particolare:

- a) identificare e censire i trattamenti di dati personali, le banche dati e gli archivi gestiti con supporti informatici e/o cartacei necessari all'espletamento delle attività istituzionalmente rientranti nella propria sfera di competenza;
- b) predisporre il registro delle attività di trattamento da esibire in caso di ispezioni delle Autorità e contenente almeno le seguenti informazioni:
 - il nome e i dati di contatto del Responsabile, del Titolare del trattamento e del Responsabile della protezione dei dati;
 - le categorie dei trattamenti effettuati;

- se del caso, i trasferimenti di dati personali verso Paesi terzi;
- descrizione delle misure di sicurezza tecniche ed organizzative applicate a protezione dei dati;
- c) definire, per ciascun trattamento di dati personali, la durata del trattamento e la cancellazione o rendere anonimi i dati obsoleti, nel rispetto della normativa vigente in materia di prescrizione e tenuta archivi;
- d) ogni qualvolta si raccolgano dati personali, provvedere a che venga fornita l'informativa ai soggetti interessati. Dovranno, inoltre, essere affissi i cartelli contenenti l'informativa, in tutti i luoghi ad accesso pubblico, con la precisazione che l'informazione resa attraverso la cartellonistica integra ma non sostituisce l'obbligo di informativa in forma orale o scritta;
- e) assicurare che la comunicazione a terzi e la diffusione dei dati personali avvenga entro i limiti stabiliti per i soggetti pubblici, ovvero, solo se prevista da una norma di legge o regolamento o se comunque necessaria per lo svolgimento di funzioni istituzionali. Così, per i dati relativi ad attività di studio e di ricerca, il Responsabile è tenuto ad attenersi alla disciplina che dispone in merito ai casi in cui è possibile la comunicazione o diffusione anche a privati di dati personali diversi da quelli sensibili e giudiziari;
- f) adempiere agli obblighi di sicurezza, quali:
 - adottare, tramite il supporto del Sistema Informativo Aziendale, tutte le preventive misure di sicurezza, ritenute idonee al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
 - definire una politica di sicurezza per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e servizi afferenti il trattamento dei dati;
 - assicurarsi la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
 - testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative applicate;
- g) far osservare gli adempimenti previsti in caso di nuovi trattamenti e cancellazione di trattamenti;
- h) collaborare con il Titolare per l'evasione delle richieste degli interessati e delle istanze del Garante per la protezione dei dati personali;
- i) collaborare alla individuazione dei soggetti terzi che trattano dati personali di cui è Titolare l'Organizzazione, ai fini della nomina in qualità di Responsabili esterni al trattamento;
- j) comunicare tempestivamente al Titolare ogni notizia rilevante ai fini della tutela della riservatezza.

Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa vigente in materia di tutela dei dati personali

relativamente al settore di competenza.

L'incarico di Responsabile del trattamento dei dati è attribuito personalmente e non è suscettibile di delega.

Ruolo di DPO nell'ambito del progetto "Sanità digitale della Regione Siciliana" - SPC CLOUD LOTTO1

Il Responsabile del trattamento dei dati personali, dovrà altresì affiancare il Cefpas nell'ambito del progetto "Sanità digitale della Regione Siciliana" - SPC CLOUD LOTTO1, fornendo supporto specialistico e consulenza relativamente alle seguenti attività:

- predisposizione degli strumenti per la conservazione dei dati sanitari trattati, che dovranno essere conformi alle normative vigenti;
- sviluppo di misure tecniche ed organizzative appropriate per proteggere i dati dei cittadini;
- verifica che i dati personali vengano trattati solo per uno scopo esplicito e legittimo e che non vengano ulteriormente trattati;
- verifica che i dati sanitari siano conservati solo per il tempo necessario allo scopo, adottando formule di anonimizzazione o cancellazione;
- accertare che il cittadino possa trasmettere i suoi dati ad altre organizzazioni, nell'ambito della medesima amministrazione, senza problemi;
- valutazione delle procedure e delle modalità con cui i cittadini possano cancellare o rettificare i propri dati sanitari, garantendo in tal modo il consenso attivo ed il diritto all'oblio;
- valutazione delle procedure di gestione dei dati, in modo che si possa certificare che i dati sensibili vengano elaborati solo se gestiti in modo sicuro (ad esempio mediante crittografia, prevenzione della perdita di dati, controlli di accesso, criteri, processo, procedure...);
- valutazione delle procedure atte a notificare alle persone qualsiasi divulgazione di dati personali senza indebito ritardo e anche ad informare le autorità di controllo entro 72 ore dall'accadimento;
- supporto nell'analisi delle normative applicabili;
- supporto nel censimento e nella classificazione dei dati sanitari;
- supporto nella definizione di un piano di sicurezza e privacy per i sistemi di interoperabilità;
- supporto nella definizione di strategie per la trasparenza e per il consenso;

FM

- determinazione e gestione del rischio informatico;

Art.2- Durata dell'incarico

L'incarico di RPD/DPO e responsabile del trattamento dati ha durata due anni, con decorrenza dalla data di sottoscrizione del presente contratto, salvo revoca motivata, (con preavviso scritto di almeno quindici giorni) o cessazione anticipata per altra causa.

In tal caso sarà dovuto il compenso maturato sino a tale data per l'incarico svolto, senza il riconoscimento di alcuna ulteriore indennità, indennizzo e/o risarcimento.

L'incarico de quo cesserà alla naturale scadenza, esclusa la proroga tacita. L'affidamento dell'incarico non determina l'instaurazione di alcun rapporto subordinato di pubblica dipendenza.

Art.3 - Compenso e liquidazione

Il valore annuale del compenso corrisposto, al lordo delle ritenute di legge, è pari ad un compenso annuo onnicomprensivo di € _____ (euro _____/00), oltre I.V.A., cassa, contributi previdenziali e assicurativi (se dovuti), da corrispondere al Responsabile Protezione Dati (RPD) / Data Protection Officer (DPO) e Responsabile del Trattamento, in rate mensili fino a completamento dell'ammontare dell'importo dovuto, dietro presentazione di regolare fattura elettronica, secondo i requisiti previsti dalla normativa vigente, unitamente ad una relazione mensile descrittiva delle attività svolte dal professionista esperto incaricato.

Il CEFPAS provvederà al pagamento entro 60 giorni dal ricevimento della fattura elettronica regolarmente emessa.

Nelle giornate di svolgimento dell'incarico il CEFPAS metterà a disposizione del professionista, l'alloggio e il pranzo di lavoro presso le strutture ricettive del Centro.

In nessun caso, ivi compreso il caso di ritardi nei pagamenti dei corrispettivi dovuti, l'incaricato potrà sospendere l'erogazione della prestazione e, comunque, lo svolgimento delle attività previste dal presente avviso. In caso di inadempienza a tale obbligo, il contratto potrà essere risolto con dichiarazione unilaterale da comunicarsi con lettera raccomandata A/R o PEC.

Art. 4 Divieto di cessione del contratto

La prestazione dovrà essere svolta personalmente dall'esperto, che potrà avvalersi di collaboratori.

Art. 5 Patto di Integrità

Il professionista dichiara di assumere gli impegni derivanti dall'integrale accettazione del Patto di Integrità approvato con Deliberazione n. 19 del 19 gennaio 2021.

Art. 6 Clausola Risolutiva Espressa

L'Amministrazione si riserva la facoltà di risolvere immediatamente e automaticamente il presente contratto, ai sensi e per gli effetti di cui all'art. 1456 del codice civile, qualora le verifiche circa il possesso dei requisiti in capo al soggetto affidatario non dovessero avere esito positivo, salvo in ogni caso il diritto dell'affidatario al pagamento delle prestazioni regolarmente eseguite.

Art. 7 Spese di contratto, di registro ed accessori

Tutte le spese inerenti e conseguenti al presente contratto, come pure i relativi tributi fiscali, eccetto l'IVA, sono a carico del professionista.

Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni generali vigenti in materia di protezione dei dati personali.

Il presente contratto è firmato e stipulato in modalità digitale in conformità al D.Lgs. n. 82/2005.

Il presente atto si compone di n. ___ pagine e viene redatto in duplice copia.

Il Responsabile del trattamento
CEFPAS

(avv. _____)

Il Titolare del trattamento – Il Direttore del

(Ing. Roberto Sanfilippo)

Ai sensi e per gli effetti di cui agli articoli 1341, 1342 codice civile si approvano specificamente le clausole apposte al contratto

Il Responsabile del trattamento
CEFPAS

(avv. _____)

Il Titolare del trattamento – Il Direttore del

(Ing. Roberto Sanfilippo)

10 / 10