Data Protection Agreement tra Titolare-Responsabile

Clausole Contrattuali Titolare – Responsabile

Scopo del Documento

Il presente documento costituisce la formulazione, aggiornata ai sensi del Reg. UE 2016/679, di un facsimile di accordo da stipulare fra Titolare e Responsabile nell'ambito di contratti o convenzioni. Tale regolazione del rapporto, può essere inserito all'interno dell'articolato dei contratti o convenzione o essere oggetto di un atto separato sottoscritto dalle parti.

Nel caso si configuri un rapporto con un terzo soggetto in qualità di sub responsabile andranno inerite le relative parti.

L'articolato può far parte di un accordo autonomo o inserito all'interno di contratti e convenzioni che regolano anche altri aspetti dei soggetti.

Il presente accordo può essere semplificato in considerazione della quantità, qualità e tipologia dei dati oggetto dei trattamenti che il Titolare demanda alla elaborazione da parte del Responsabile.

Definizioni:

Titolare il soggetto titolare delle finalità dei trattamenti e dei dati personali oggetto delle attività disciplinate dal contratto/convenzione

Responsabile il soggetto che effettua trattamenti di dati personali per conto del Titolare

Interessato la persona fisica cui si riferiscono i dati personali trattati

DPO Responsabile trattamento dati personali/Data Protection Officer

GDPR Regolamento Europeo sulla protezione dei dati personali 679/2016 – General Data Protection Regulation

CISO la persona o la struttura a cui sono demandate le attività di auditing sulle misure di sicurezza adottate e di incident management

Incident management procedura di gestione degli incidenti IT relativi a dati personali

Responsabile della sicurezza IT la persona o la struttura cui è demandato il compito di definire, impostare e gestire le misure di sicurezza IT

Lock-In con tale termine si intende la diminuzione o perdita da parte del titolare della possibilità di gestire i servizi e relativi dati in autonomia senza dover forzatamente ricorrere al soggetto a cui ne ha ceduto la gestione. La sicurezza dei dati e la continuità del servizio devono sempre essere sotto il controllo del Titolare.

Accordo Data Protection fra Titolare, Responsabile
(Data Protection Agreement)

TRA

Regione Toscana, con sede legale in Firenze, Piazza Duomo 10, in persona del delegato del Titolare ai sensi della DGR 585/2018 Ing. Gianluca Vannuccini, Direttore Sistemi Informativi, infrastrutture Tecnologiche e Innovazione

E

Il _____, residente a _____, C.F. _____

Visti:

Il Decreto del Presidente del Consiglio dei Ministri recante "Riparto delle risorse per il conferimento di incarichi di collaborazione per il supporto ai procedimenti amministrativi connessi all'attuazione del PNRR" del 12 novembre 2021, pubblicato sulla Gazzetta Ufficiale n. 284 del 29 novembre 2021;

La delibera n. 1286 del 6/12/2021 con la quale la Giunta regionale ha approvato il Piano Territoriale della Regione Toscana, trasmesso al Dipartimento della Funzione pubblica con nota protocollo AOOGRT0463045B.080.020 del 29/11/2021;

Il Decreto Dirigenziale n _____ del _____ " CUP D51B21004050006_____" con il quale l'Ing. _____ è stato incaricato con Contratto di collaborazione professionale ad esperto PNRR - Esperto profilo professionale *Ingegnere Informatico/Ingegnere Gestionale* Task Force "Digitalizzazione e Architetture IT" dal 01/01/2023 al 31/12/2024.

Dato Atto che il contratto sopra citato specifica che l'Esperto è tenuto ad osservare la massima riservatezza su informazioni, documenti o altro tipo di materiale prodotto direttamente dall'amministrazione ovvero proveniente da altre amministrazioni o altri soggetti, di cui viene in possesso nell'espletamento dell'incarico, nonché sui risultati, anche parziali, della propria attività, in qualsiasi forma (cartacea, informatica, ecc.), fatto salvo il caso in cui Regione Toscana ne disponga, previo assenso dell'altra Parte, la diffusione secondo le modalità ritenute più opportune.

ART. 1 TRATTAMENTO DEI DATI PERSONALI

Ai sensi e per gli effetti della normativa in materia di protezione dei dati personali (Reg. UE n. 2016/679, di seguito "GDPR", nonché D. Lgs. 196/2003 da ultimo novellato dal D. Lgs. 101/2018, di seguito "Codice Privacy"), ed in relazione alle operazioni che vengono eseguite per lo svolgimento delle attività previste dal Contratto di cui al Decreto Dirigenziale n. 22794 del 24.12.2021 e dai relativi allegati, oltre che dal Piano di attività di dettaglio concordato con l'Amministrazione Regionale, il **Direttore Ing. Gianluca Vannuccini in qualità di Titolare**, nomina **L'Ing. _____ Responsabile del trattamento**, ai sensi dell'articolo 28 GDPR.

Titolare e Responsabile verranno in seguito entrambi indicati congiuntamente "le Parti".

I trattamenti affidati dal Titolare al Responsabile riguardano:

- tipologia dei dati personali: dati enti locali, dati delle aziende e strutture sanitarie, delle istituzioni della ricerca, delle aziende, delle associazioni e dei soggetti individuali coinvolti nelle attività previste dal contratto e dal piano di attività;
- categorie degli interessati: professionisti, titolari e rappresentanti legali delle aziende, personale dipendente delle aziende interessate, dipendenti delle amministrazioni;
- tipologia del formato dei dati: dati in formato testuale

I trattamenti effettuati per conto del Titolare dal Responsabile cesseranno alla conclusione del Contratto citato in premessa, ovvero in caso di risoluzione per qualsiasi altro motivo.
Se una disposizione del presente articolo è, o diventa invalida o inapplicabile, la validità e l'applicabilità delle altre disposizioni del medesimo rimangono inalterate. In questo caso, Titolare e Responsabile concordano di adottare una disposizione che corrisponda al meglio allo scopo previsto nella disposizione non valida o agli interessi comuni.

L'Ing. _____ Esperto, in quanto Responsabile, fornisce garanzie sufficienti, in particolare in termini di conoscenze specialistiche, affidabilità e risorse, per attuare misure tecniche e organizzative che soddisfino i requisiti normativi sanciti dal GDPR, dal Codice Privacy e da qualsiasi altra norma connessa inerente al trattamento dei dati personali, comprese le misure di sicurezza del trattamento, per garantire la riservatezza e la protezione dei diritti degli interessati.
L'Ing. _____ Esperto, in quanto Responsabile, è tenuto ad assicurare la riservatezza ed il corretto trattamento delle informazioni, dei documenti e degli atti amministrativi, dei quali venga a conoscenza durante l'esecuzione della prestazione.

In particolare, ai sensi dell'art. 28 GDPR, il Responsabile si impegna a:

- non mettere in atto, per nessun motivo, trattamenti di dati diversi da quelli autorizzati dal Titolare oggetto del presente accordo;
- non diffondere i dati oggetto del trattamento ad altri soggetti esterni alle attività di progetto previste nel Contratto citato in premessa e non esporli in pubblicazioni o in rete;
- collaborare alla eventuale redazione di DPIA su trattamenti affidati alla sua responsabilità dal Titolare;
- predisporre e trasmettere al Titolare, con cadenza annuale e comunque ogni qualvolta ciò appaia necessario, una relazione in merito agli adempimenti eseguiti e alle misure di sicurezza adottate al fine di renderle e mantenerle sempre adeguate ed aggiornate rispetto alla evoluzione delle minacce e sulla base dei riscontri derivanti dalla registrazione continua e puntuale degli incidenti eventualmente occorsi;
- assistere e garantire il Titolare del trattamento nell'evasione delle richieste e del rispetto dei tempi previsti, nei rapporti con l'Autorità Garante per la protezione dei dati personali;
- assistere il Titolare al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati ai sensi degli artt. 15 a 22 del Regolamento UE; qualora gli interessati esercitino tale diritto verso il Responsabile, quest'ultimo è tenuto ad inoltrare tempestivamente e comunque nel più breve tempo possibile, le istanze al Titolare, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei tempi prescritti
- assistere ed assicurare la piena, fattiva e puntuale collaborazione al Titolare del trattamento, ed in particolare al CISO del Titolare se nominato, nel garantire il rispetto degli obblighi di

cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento, della tipologia di dati trattati, delle categorie e numerosità degli interessati.

- garantire al Titolare, su richiesta, l'accesso e la disponibilità permanente ai dati, su formati e strumenti di uso comune che ne garantiscano la fruizione da parte del Titolare, consentendo in tal modo la piena continuità dei servizi oggetto del presente appalto e in modo che mai si configuri una situazione di lock in. Il Titolare deve essere sempre messo in condizione di poter garantire la continuità del servizio;
- restituire tutti i dati personali di pertinenza del Titolare, dopo che è terminata la prestazione dei servizi relativi al trattamento, cancellando le copie esistenti in proprio possesso, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati. In tal caso il Titolare e il Responsabile concordano modalità, tempi e forme idonee a garantire il non precostituirsi di situazioni di lock in, inteso come la diminuzione o perdita della possibilità da parte del Titolare di garantire i servizi, senza ricorrere forzatamente al soggetto Responsabile, e di gestire agevolmente, in modo sicuro e con tempi ragionevoli, la chiusura dell'accordo e l'eventuale subentro di un nuovo contraente o la gestione in autonomia in toto o in parte dei servizi. Tale accordo documentato viene messo a disposizione del Titolare e del DPO della Giunta regionale;
- mettere in atto gli interventi necessari qualora l'attività di monitoraggio e controllo mettesse in evidenza punti di debolezza nelle misure e nelle tecniche adottate o qualora durante la vigenza del presente Accordo, la normativa in materia di Trattamento dei Dati Personali generi nuovi requisiti (ivi incluse nuove misure di natura fisica, logica, tecnica, organizzativa, in materia di sicurezza o trattamento dei dati personali), il Responsabile del trattamento si impegna a collaborare - nei limiti delle proprie competenze tecniche, organizzative e delle proprie risorse - con il Titolare affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento deve mettere in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. Tali misure comprendono tra le altre, se del caso:

a. la capacità di assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi che trattano i dati personali;
b. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
c. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

A tal fine si impegna ad assistere ed assicurare la piena, fattiva e puntuale collaborazione al Titolare del trattamento, ed in particolare al CISO del Titolare.

Il Responsabile informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, il Titolare di ogni violazione di dati personali (cd. data breach); tale notifica è accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del Regolamento UE, per permettere al Titolare del trattamento, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto il Titolare ne viene a conoscenza; nel caso in cui il Titolare debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità di controllo siano esclusivamente in possesso del Responsabile.

Sarà obbligo del Titolare del trattamento vigilare durante tutta la durata del trattamento, sul rispetto degli obblighi previsti dalle presenti istruzioni e dal Regolamento UE sulla protezione dei dati da parte del Responsabile del trattamento, nonché a supervisionare l'attività di trattamento dei dati personali anche effettuando, se del caso, audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile. A tal fine il Responsabile del trattamento metterà a disposizione, su richiesta del titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi derivanti dal regolamento UE, agevolando il contributo alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato, ivi compresa, se necessario, l'attività di monitoraggio e controllo da parte del DPO e del CISO del Titolare, sulle misure di sicurezza attuate e sulla loro efficacia fornendo tutta la documentazione che sarà richiesta e collaborando attivamente alle attività di rilevazione e misura.

ART 2 – ISTRUZIONI PER IL RESPONSABILE AI FINI DEL TRATTAMENTO DATI SU SUPPORTO INFORMATICO O CARTACEO O TRAMITE SISTEMI INFORMATICI

- Ai fini del presente documento, si intende con "Sistema Informatico" qualunque sistema informatico in cui la Regione Toscana abbia inserito banche dati o porzioni di esse.
- In caso di necessità di accesso ai Sistemi Informatici Regionali, vengono consegnate al Responsabile le credenziali di autenticazione che consentono l'accesso al sistema mediante una procedura di autenticazione basata che identifica univocamente al Responsabile. Tali credenziali hanno carattere strettamente individuale e non devono essere comunicate o rese conoscibili da altri.
- La componente riservata delle credenziali (ad esempio la password) deve essere conservata segretamente dal Responsabile; eventuali dispositivi contenenti la parte riservata delle credenziali (cd-card, smart-card, o altro supporto di memorizzazione) devono essere custoditi con la massima cura in luogo chiuso a chiave.
- Ogni Responsabile che utilizzerà un Sistema Informatico Regionale dovrà adottare opportune cautele per proteggere il sistema durante la sua assenza dalla sessione di trattamento, con uso della parola chiave all'avvio della sessione di lavoro e per lo screen-saver.
- In caso di prolungata assenza o impedimento del Responsabile del trattamento dei dati sul Sistema Informatico, le credenziali associate al Responsabile saranno rese inutilizzabili.
- I dati documenti informatici o su supporto informatico, relativi a dati personali devono essere conservati dal Responsabile in archivi chiusi; gli accessi tramite computer devono essere protetti da password.
- I sistemi informatici (computer, smartphone e sistemi di mantenimento dei dati, o similari) utilizzati dal responsabile per il trattamento dei dati devono essere accessibili con password o altri sistemi di controllo degli accessi e dotati di opportuni sistemi che li proteggano da accessi non consentiti, anche tramite la rete.
- In caso di spedizione dei documenti a soggetti autorizzati al trattamento nell'ambito del contratto citato in premessa, qualunque sia il tipo di spedizione adottato, si deve porre cura di accertare il corretto destinatario e che lo stesso abbia effettivamente ricevuto i documenti inviati e che essi sono giunti integri, e quindi non manomessi o alterati in fase di trasporto.
- I documenti contenenti dati personali devono essere custoditi in un luogo sicuro; tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò sia assolutamente necessario, l'asportazione deve essere ridotta al minimo tempo occorrente per effettuare le operazioni di trattamento.

- Dal luogo sicuro devono essere asportati solo i documenti strettamente necessari per le operazioni di trattamento e non intere pratiche, se ciò non sia necessario.
- Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro
- Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, il Responsabile non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
- L'incaricato deve inoltre controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando sia il numero dei fogli che l'integrità del contenuto.
- I documenti di cui sopra non devono essere mai lasciati incustoditi durante l'attività lavorativa.
- Se si debbono abbandonare, al termine dell'attività o durante pause, gli anzidetti documenti, il Responsabile deve identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio chiuso a chiave, un cassetto chiuso a chiave, una cassaforte, un armadio blindato, un classificatore chiuso a chiave); ove si utilizzi un contenitore chiuso a chiave, di qualunque natura, occorre accertarsi che non esistano duplicati abusivi delle chiavi e che tutte le chiavi siano in possesso solo di incaricati autorizzati.
- Ci si deve accertare che un visitatore o terzo che entri nella sede di lavoro, anche non invitato o per cause accidentali, non venga a conoscenza dei contenuti dei documenti.
- Si deve limitare al minimo il numero di fotocopie effettuate, non diffonderle a terzi non autorizzati e porre attenzione all'utilizzo di macchine fotocopiatrici di ultima generazione, che siano in grado di catturare l'immagine del documento e/o conservare il file elettronico dello stesso. In questo caso la fotocopiatrice va classificata come strumento elettronico e si applicano pertanto le particolari cautele, previste per questa tipologia di strumenti.
- Eventuali fotocopie non riuscite bene debbono essere distrutte mediante apposito distruggitore, se disponibile, oppure devono essere strappate in pezzi talmente piccoli da non consentire in alcun modo la ricostruzione del contenuto.
- È parimenti tassativamente proibito utilizzare come carta per appunti o trasportare all'esterno del posto di lavoro fotocopie non riuscite.
- Si deve adottare una procedura per la consegna delle copie ai destinatari che dia tutte le garanzie di sicurezza necessarie a ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto delle stesse o fotocopiarlo all'insaputa del mittente e destinatario.
- Qualora i documenti debbano essere trasportati all'esterno del luogo di lavoro, il Responsabile deve tenere sempre con sé la cartella o la borsa contenente i documenti e deve evitare che sia possibile esaminare, da parte di soggetti terzi non autorizzati, anche solo la copertina della cartella contenente i documenti.
- Durante il trasporto, la cartella non deve essere lasciata incustodita e la cartella o valigia ove possibile deve essere tenuta chiusa a chiave o ne devono essere azionate le serrature a combinazione.
- In caso di dubbio sulle modalità di applicazione di quanto sopra illustrato l'incaricato deve rivolgersi al Titolare.

ART 3 – INADEMPIENZE

Eventuali controversie che dovessero insorgere legate alla possibilità che il Responsabile possa aver agito in modo difforme o contrario alle legittime istruzione del Titolare oppure abbia adottato misure

di sicurezza inadeguate rispetto al rischio del trattamento, saranno risolte, in prima istanza, secondo procedimento amichevole tra le Parti tramite richiesta da parte del Titolare di apertura di una procedura di conciliazione della controversia. Un referente del Titolare (il DPO, se nominato) e un referente del Responsabile porteranno avanti la composizione della controversia in tempi ragionevoli. Qualora dopo aver esperito ogni tentativo di conciliazione, la controversia non venga risolta entro 30 giorni dall'avvio della procedura, e venga altresì comprovata la causa esclusiva di inadempienza da parte del Responsabile, questi risponderà del danno causato agli "interessati" e il Titolare potrà risolvere il contratto, salvo il risarcimento del maggior danno.

Il Titolare	**Il Responsabile del trattamento**
Ing. Gianluca Vannuccini	**Ing. _____**