NOMINA RESPONSABILE DEL TRATTAMENTO DEI DATI

- Con la sottoscrizione della presente da parte dell'Amministrazione dell'Amministrazione **ARIC - AGENZIA REGIONALE DI INFORMATICA E COMMITTENZA** con sede in Via Napoli n. 4 – 64019 Tortoreto Lido (TE) in persona del legale rappresentante Avv. Donato Cavallo, il Fornitore Telecom Italia S.p.A. - rappresentato dal procuratore Dr. Gaspare Monastero che sottoscrive per accettazione, è nominato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE n. 2016/679 sulla protezione delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (nel seguito anche "Regolamento UE"), per tutta la durata del contratto esecutivo n. ***2291022630676003COE*** (nel seguito anche "contratto"), nell'ambito del Contratto Quadro per l'affidamento dei servizi di cloud computing per le Pubbliche Amministrazioni – Lotto 1. A tal fine il Responsabile è autorizzato a trattare i dati personali necessari per l'esecuzione delle attività oggetto del contratto e si impegna ad effettuare, per conto dell'Amministrazione (Titolare del trattamento), le sole operazioni necessarie per fornire il servizio oggetto del contratto, nei limiti delle finalità ivi specificate, nel rispetto del Codice Privacy, del Regolamento UE (nel seguito anche "Normativa in tema di trattamento dei dati personali") e delle istruzioni nel seguito fornite.
- Il Fornitore/Responsabile si impegna a presentare, su richiesta dell'Amministrazione, garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse per l'adozione di misure tecniche ed organizzative adeguate volte ad assicurare che il trattamento sia conforme alle prescrizioni della normativa in tema di trattamento dei dati personali.
- **Le finalità del trattamento sono:**

  i) supporto alla gestione documentale e mantenimento database utenti con dati sensibili;

  ii) supporto alla gestione infrastrutture e piattaforme ICT
- **Il tipo di dati personali trattati in ragione delle attività oggetto del contratto sono: i) dati comuni (database utenti); ii) dati sensibili; iii) dati sanitari.**
- **Il Responsabile dichiara che il trattamento dei dati verrà effettuato in Italia.**
- **Le categorie di interessati sono:**

  i) dipendenti; ii) collaboratori; iii) professionisti; iv) cittadini
- Nell'esercizio delle proprie funzioni, il Responsabile si impegna a:

  a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;

  b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;

c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate che il Fornitore si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del contratto, d'ora in poi "persone autorizzate"; nel caso in cui ritenga che un'istruzione costituisca una violazione del Regolamento UE sulla protezione dei dati o delle altre disposizioni di legge relative alla protezione dei dati personali, il Fornitore deve informare immediatamente l'Amministrazione;

d) garantire la riservatezza dei dati personali trattati nell'ambito del contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del contratto:

   - si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
   - ricevano la formazione necessaria in materia di protezione dei dati personali;
   - trattino i dati personali osservando le istruzioni impartite dal Titolare per il trattamento dei dati personali al Responsabile del trattamento;

e) adottare politiche interne e attuare misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design), nonché adottare misure tecniche ed organizzative adeguate per garantire che i dati personali siano trattati, in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il periodo strettamente necessario al raggiungimento delle stesse (privacy by default);

f) adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;

g) su eventuale richiesta dell'Amministrazione, assistere quest'ultima nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente all'articolo 35 del Regolamento UE e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'articolo 36 del medesimo Regolamento UE;

h) adottare le misure minime di sicurezza ICT per le PP.AA. di cui alla Circolare AgID n. 2/2017 del 18 aprile 2017, nelle modalità indicate nei documenti programmatici di sicurezza riportati in calce;

i) ai sensi dell'art. 30 del Regolamento UE, e nei limiti di quanto esso prescrive tenere un Registro delle attività di trattamento effettuate sotto la propria responsabilità e cooperare con l'Amministrazione e con l'Autorità Garante per

la protezione dei dati personali, mettendo il predetto Registro a disposizione dell'Amministrazione e dell'Autorità, laddove ne venga fatta richiesta ai sensi dell'art. 30 comma 4 del Regolamento UE;

Ferme restando le misure di sicurezza indicate nei documenti programmatici di sicurezza riportati in calce, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, il Responsabile del trattamento su richiesta dell'Amministrazione e previo accordo tra le parti, potrà fornire misure di sicurezza integrative (nel rispetto dell'oggetto contrattuale) , che saranno concordate al fine di mettere in atto misure tecniche ed organizzative idonee per garantire un livello di sicurezza adeguato al rischio e per garantire il rispetto degli obblighi di cui all'art. 32 del Regolamento UE. La valutazione circa l'adeguatezza del livello di sicurezza deve tenere conto, in particolare, dei rischi del trattamento derivanti da: distruzione o perdita anche accidentale, modifica, divulgazione non autorizzata, nonché accesso non autorizzato, anche accidentale o illegale, o trattamento non consentito o non conforme alle finalità del trattamento dei dati personali conservati o comunque trattati.

- Il Responsabile del trattamento deve mettere a disposizione dell'Amministrazione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento UE, oltre a contribuire e consentire all'Amministrazione - anche tramite soggetti terzi dal medesimo autorizzati, dandogli piena collaborazione - verifiche periodiche, ispezioni e audit circa l'adeguatezza e l'efficacia delle misure di sicurezza adottate ed il pieno e scrupoloso rispetto delle norme in materia di trattamento dei dati personali. A tal fine, l'Amministrazione informa preventivamente il Responsabile del trattamento con un preavviso minimo di sei giorni lavorativi.
- Nel caso in cui all'esito di tali verifiche periodiche, ispezioni e audit le misure di sicurezza dovessero risultare inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Fornitore agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima diffiderà il Fornitore ad adottare tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a seguito della diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà, in ragione della gravità della condotta del Fornitore e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.
- In alternativa alle verifiche di cui sopra, l'Amministrazione potrà richiedere al Responsabile di fornire annualmente o comunque su richiesta dell'Amministrazione una relazione sull'andamento della gestione dei dati personali e sull'applicazione delle misure di sicurezza approvate.

- Il Responsabile/Sub Responsabile può ricorrere a Sub Responsabili/Terzi autorizzati per gestire le attività di trattamento. A tal fine il Responsabile/Sub responsabile rende disponibile all'Amministrazione l'elenco aggiornato dei sub Responsabili/Terzi autorizzati, contenuto nel/i documento/i programmatico di sicurezza riportato in calce. Nell'elenco sono altresì specificate le attività di trattamento delegate, i dati identificativi del sub-Responsabile e i dati del contratto eseguito da terze parti. Tale elenco verrà aggiornato in caso di modifiche riguardanti l'aggiunta o la sostituzione di sub Responsabili.
- In caso di variazioni del/dei documento/i riportati in calce il Responsabile/Sub Responsabile si impegna a comunicare la nuova versione tramite PEC entro 10 giorni dalla sua approvazione da parte del Comitato di Direzione Tecnica.
- L'Amministrazione avrà la facoltà motivata di opporsi, in relazione all'attribuzione dello specifico trattamento ad un determinato Sub Responsabile/Terzo Autorizzato aggiunto in caso di aggiornamento dell'elenco di cui sopra in corso di esecuzione del Contratto Esecutivo, chiedendone la sostituzione.
- Il sub-Responsabile del trattamento deve rispettare obblighi analoghi a quelli forniti dall'Amministrazione al Responsabile Iniziale del trattamento <oppure sub-Responsabile del trattamento>, riportate in uno specifico contratto o atto di nomina. Spetta al Responsabile Iniziale assicurare che il sub-Responsabile del trattamento presenti garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per l'adozione di misure tecniche ed organizzative appropriate di modo che il trattamento risponda ai principi e alle esigenze del Regolamento UE.
- In caso di violazione da parte del sub-Responsabile del trattamento degli obblighi in materia di protezione dei dati, il Responsabile Iniziale del trattamento è interamente responsabile nei confronti dell'Amministrazione del trattamento di tali inadempimenti. L'Amministrazione potrà in qualsiasi momento verificare le garanzie e le misure tecniche ed organizzative del sub-Responsabile, tramite audit verifiche e ispezioni anche avvalendosi di soggetti terzi. A tal fine, l'Amministrazione informa preventivamente il Responsabile del trattamento con un preavviso minimo di sei giorni lavorativi.
- Ove tali misure dovessero risultare inapplicate o inadeguate rispetto al rischio del trattamento o, comunque, inidonee ad assicurare l'applicazione del Regolamento, o risulti che il Sub responsabile/terzo autorizzato agisca in modo difforme o contrario alle istruzioni fornite dall'Amministrazione, quest'ultima diffiderà il Fornitore a far adottare al sub-Responsabile del trattamento tutte le misure più opportune o a tenere una condotta conforme alle istruzioni entro un termine congruo che sarà all'occorrenza fissato. In caso di mancato adeguamento a tale diffida, resa anche ai sensi dell'art. 1454 cc, l'Amministrazione potrà, in ragione della gravità della condotta del sub responsabile/terzo autorizzato e fatta salva la possibilità di fissare un ulteriore termine per l'adempimento, risolvere il contratto

con il Responsabile iniziale ed escutere la garanzia definitiva, salvo il risarcimento del maggior danno.

- Restano fermi i casi di recesso previsti nel Contratto Quadro.
- In alternativa alle verifiche di cui sopra, l'Amministrazione potrà richiedere al Responsabile di fornire annualmente o comunque su richiesta dell'Amministrazione una relazione sull'andamento della gestione dei dati personali e sull'applicazione delle misure di sicurezza approvate da parte del subResponsabile/terzo autorizzato.
- Il Responsabile del trattamento manleverà e terrà indenne l'Amministrazione da ogni perdita, contestazione, responsabilità, spese sostenute nonché dei costi subiti (anche in termini di danno reputazionale) in relazione anche ad una sola violazione della normativa in materia di Trattamento dei Dati Personali e/o del Contratto (inclusi gli Allegati) derivata dalla condotta (attiva e/o omissiva) sua e/o dei suoi agenti e/o sub appaltatori e/o sub-contraenti .
- Il Fornitore Responsabile del trattamento deve assistere l'Amministrazione al fine di dare seguito alle richieste per l'esercizio dei diritti degli interessati; qualora gli interessati esercitino tale diritto presso il Responsabile del trattamento, quest'ultimo è tenuto ad inoltrare tempestivamente, e comunque nel più breve tempo possibile, le istanze all'Amministrazione, supportando quest'ultimo al fine di fornire adeguato riscontro agli interessati nei termini prescritti.
- Il Fornitore Responsabile del trattamento informa tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, l'Amministrazione 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 all'Amministrazione, ove ritenuto necessario, di notificare questa violazione all'Autorità Garante per la protezione dei dati personali, entro il termine di 72 ore da quanto l'Amministrazione ne viene a conoscenza; nel caso in cui l'Amministrazione debba fornire informazioni aggiuntive all'Autorità di controllo, il Responsabile del trattamento si impegna a supportare l'Amministrazione nell'ambito di tale attività.
- Il Fornitore Responsabile del trattamento deve avvisare tempestivamente e senza ingiustificato ritardo l'Amministrazione in caso di ispezioni, di richiesta di informazioni e di documentazione da parte dell'Autorità Garante per la protezione dei dati personali; inoltre, deve assistere l'Amministrazione nel caso di richieste formulate dall'Autorità Garante in merito al trattamento dei dati personali effettuate in ragione del contratto.
- Il Fornitore Responsabile del trattamento deve comunicare all'Amministrazione i dati di contatto del proprio "Responsabile della protezione dei dati", qualora, in ragione dell'attività svolta, ne abbia designato uno conformemente all'articolo 37 del Regolamento UE; il Responsabile della protezione dei dati personali del Fornitore/Responsabile collabora e si tiene in costante contatto con il Responsabile della protezione dei dati dell'Amministrazione. I dati di contatto del DPO del

Responsabile/Sub Responsabile sono disponibili nel/i documento/i programmatico/i di sicurezza riportato/i in calce.

- Al termine della prestazione dei servizi oggetto del contratto, il Responsabile su richiesta dell'Amministrazione, si impegna a: i) restituire all'Amministrazione i supporti rimovibili eventualmente utilizzati su cui sono memorizzati i dati; ii) distruggere tutte le informazioni registrate su supporto fisso, documentando per iscritto l'adempimento di tale operazione.
- Il Fornitore si impegna a individuare e a designare per iscritto gli amministratori di sistema mettendo a disposizione dell'Amministrazione l'elenco aggiornato delle nomine.
- Il Responsabile del trattamento si impegna ad operare adottando tutte le misure tecniche e organizzative, le attività di formazione, informazione e aggiornamento ragionevolmente necessarie per garantire che i Dati Personali trattati in esecuzione del contratto, siano precisi, corretti e aggiornati nel corso della durata del trattamento - anche qualora il trattamento consista nella mera custodia o attività di controllo dei dati - eseguito dal Responsabile, o da un sub-Responsabile.
- Il Responsabile non può trasferire i dati personali verso un paese terzo o un'organizzazione internazionale salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte dell'Amministrazione.
- Sarà obbligo dell'Amministrazione 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 effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile del trattamento.
- Durante l'esecuzione del Contratto, nell'eventualità di qualsivoglia modifica della normativa in materia di Trattamento dei Dati Personali che 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 l'Amministrazione affinché siano sviluppate, adottate e implementate misure correttive di adeguamento ai nuovi requisiti.

***

Si precisa che:

a) Sulla sezione riservata del portale www.cloudspc.it è pubblicato il Documento "Documento Programmatico di gestione della Sicurezza dei Servizi Cloud TIM SPC", revisione 7 del 28/10/2020, sottoscritto digitalmente dal procuratore speciale Santocchia Giovanni (il "Documento Programmatico della Sicurezza TIM" o il "DPS TIM");

b) Sulla sezione riservata del portale www.cloudspc.it è pubblicato il Documento di Telecom Italia "Documento Programmatico della Sicurezza Servizio di Conservazione – SPC Lotto1", codice documento CONSPRIN.TT.DPS16000.01 emesso a dicembre 2018, sottoscritto digitalmente dal procuratore speciale Santocchia Giovanni (il "Documento Programmatico della Sicurezza di Trust Technologies" o il "DPS Trust").

c) Sulla sezione riservata del portale www.cloudspc.it è pubblicato il Documento di Enterprise Services "Documento Generale della Sicurezza e Privacy", codice documento DGSP ES emesso il 26.02.2019, sottoscritto digitalmente dal Legale Rappresentante Lorenzo Greco (il "Documento Generale della Sicurezza e Privacy ES" o il "DGSP ES").

d) Sulla sezione riservata del portale www.cloudspc.it è pubblicato il Documento di Postel "Documento Programmatico della Sicurezza SPC Cloud Computing Servizio di conservazione digitale", versione 1.0 emesso il 21/02/2019, sottoscritto digitalmente dal procuratore speciale Fabio Gambino (il "Documento Programmatico della Sicurezza Postel" o il "DPS Postel").

Letto, approvato e sottoscritto

L'AMMINISTRAZIONE

Direttore Generale - Avv. Donato Cavallo

C.F.: CVLDNT72D16H703P

Firmato digitalmente da: DONATO CAVALLO
Ruolo: DIRETTORE GENERALE ARIC
Data: 19/05/2022 13:40:00

IL FORNITORE

Dr. Gaspare Monastero

C.F.: MNSGPR65S23C696V
Certificatore: TI Trust Technologies CA
Validità: dal 13/07/2020 al 13/07/2023
Seriale Certificato: 724143