ALLEGATO B: ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO AI SENSI DELL'ARTICOLO 28 DEL REGOLAMENTO (UE) N. 2016/679

Oggetto: Attribuzione del ruolo di responsabile del trattamento, ai sensi dell'articolo 28 del Regolamento Europeo n. 2016/679 – CONVENZIONE PER LA COLLABORAZIONE NELLA GESTIONE DEL RECEPIMENTO DELLE ISTANZE DI BONUS TLR 2023 PRESENTATE DA CLIENTI DOMESTICI ECONOMICAMENTE SVANTAGGIATI del __/___/_____

TRA

IREN Mercato S.p.A. con sede legale in Via SS. Giacomo e Filippo n. 7 – 16122 Genova, (nel seguito anche brevemente "**IREN**" o il "**Committente**") in persona del procuratore *pro tempore*

E

_____, con sede legale in **[XXX]**, (nel seguito anche brevemente "**Fornitore**"), in persona del socio-procuratore, munito dei relativi poteri.

Di seguito denominate congiuntamente anche le "Parti".

Premesso che[1]:

- il presente atto di nomina ha lo scopo di disciplinare i rapporti tra le Parti in relazione al trattamento dei dati personali da parte del Fornitore. A tal fine, in ragione delle diverse modalità nelle quali può estrinsecarsi la titolarità/responsabilità di IREN circa il trattamento dei dati personali, potranno aversi le seguenti casistiche applicabili (da indicare):

☒ IREN svolge trattamento di dati personali di cui è titolare ed intende procedere, ai sensi dell'art. 28 del Regolamento (UE) n. 679/2016 (nel seguito, per brevità, indicato come "GDPR"), alla attribuzione al Fornitore del ruolo di responsabile esterno per il trattamento dei suddetti dati personali ("**Ipotesi 1**");

☐ IREN è responsabile del trattamento dei dati personali, ai sensi dell'art. 28 del GDPR la cui titolarità è ascrivibile ad altre entità appartenenti al Gruppo IREN identificate nell'Allegato B al presente atto ("**Entità del Gruppo IREN**"); a fronte di ciò, intende procedere all'attribuzione al Fornitore del ruolo di altro responsabile del trattamento dei suddetti dati personali ai sensi dell'art. 28 del GDPR, paragrafo 4 ("**Ipotesi 2**");

☐ IREN svolge attività di trattamento dei dati personali in qualità di titolare autonomo del trattamento e, contestualmente, per conto di altre Entità del Gruppo IREN identificate nell'Allegato B al presente atto in qualità di Responsabile Esterno del trattamento; in tale contesto, s'intende procedere alla nomina del Fornitore quale Responsabile Esterno del trattamento per il trattamento di dati in titolarità di IREN e Altro Responsabile Esterno per il trattamento di dati personali in titolarità di altre Entità appartenenti al Gruppo IREN ("**Ipotesi 3**").

- il Fornitore s'impegna a svolgere le attività di cui all'oggetto della Convenzione _____ del___/___/_____ (nel seguito il "**Contratto**")[2] tra IREN (in nome proprio ovvero in nome e per conto delle altre Entità del Gruppo IREN) ed il Fornitore (nel seguito l'"**Incarico**");
- lo svolgimento dell'Incarico comporta il trattamento di dati personali, di IREN e/o di altre Entità del Gruppo IREN, ai sensi e per gli effetti di quanto disciplinato dal GDPR e dal Decreto Legislativo 30 giugno 2003, n. 196 così come novellato dal Decreto Legislativo 10 agosto 2018, n. 101 (nel seguito, per brevità, indicate congiuntamente come "Norme in materia di Protezione dei Dati Personali");
- il Fornitore garantisce di essere in possesso di adeguata esperienza, capacità e professionalità in misura tale da garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati

1 Al fine di identificare compiutamente la corretta qualificazione giuridica del rapporto di gestione del trattamento tra le Parti, si prega di identificare la casistica corrispondente.

2 Si prega di indicare il documento contrattuale di riferimento

personali, ivi compresa l'applicazione del GDPR e dalle Norme in materia di protezione dei Dati Personali;

- il Fornitore intende agire per il trattamento di dati personali, necessari ai fini dell'Incarico, a mezzo dei propri incaricati[3] al trattamento dei dati personali (di seguito "Incaricati"), ai quali sono state impartite le relative istruzioni la cui puntuale applicazione verrà verificata periodicamente;
- IREN intende procedere alle summenzionate attribuzioni del ruolo di responsabile del trattamento, come disciplinate dall'art. 28 del GDPR, unificando i termini e le condizioni con le quali il Fornitore viene incaricato del trattamento;
- Le summenzionate attribuzioni sono da intendersi quali limitate all'ambito dell'Incarico, con riferimento al trattamento di seguito indicato:

Nome del/dei trattamento/i	Gestione erogazione bonus TLR
Descrizione del/dei trattamento/i	Il Fornitore svolge per conto del Titolare la gestione delle attività di recepimento e valutazione delle istanze di accesso al bonus TLR da parte dei singoli utenti. I cittadini possono presentare domanda (anche utilizzando modalità di identificazione tramite SPID e CIE) al Comune di residenza corredata di ISEE, copia documenti di identità e codice fiscale, bolletta del TLR (se contratto individuale), autocertificazione composizione nucleo famigliare.
Finalità del trattamento	Erogazione del bonus TLR
Dati personali trattati per conto di Iren	Dati personali comuni - anagrafici e di contatto Dati personali comuni - Dati anagrafici di stato civile Dati personali comuni - Dati contrattuali Dati personali comuni - Dati tecnici Dati personali comuni - Dati economico-finanziari-patrimoniali Dati personali comuni - Dati di fatturazione
Categorie di interessati al trattamento dei dati	Clienti
Durata del/i trattamento/i	Fino al termine del contratto ed in conformità agli eventuali adempimenti normativi applicabili

Premesso quanto sopra,
le Parti convengono di vincolarsi, ai fini del trattamento dei dati personali in questione, a quanto segue:

con la sottoscrizione del presente atto il Fornitore viene incaricato, a seconda delle attività di trattamento identificata al punto I delle Premesse:

3 Ai fini del presente atto di attribuzione del ruolo per la disciplina del trattamento dei dati personali, con il termine "Incaricato" si intende qualsiasi "persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" come previsto agli articoli 4, numero 10, e 29 del GDPR.

1. nel caso di applicabilità dell'**Ipotesi 1**, quale Responsabile Esterno, ai sensi dell'articolo 28 del GDPR, del trattamento di dati personali di cui IREN è titolare, ai fini dell'Incarico e nei termini ed alle condizioni che seguono.
2. nel caso di applicabilità dell'**Ipotesi 2**, quale Altro Responsabile esterno ai sensi dell'articolo 28, paragrafo 4, del GDPR, del trattamento di dati personali di cui IREN è Responsabile Esterno del trattamento, ai fini dell'Incarico e nei termini ed alle condizioni che seguono;
3. nel caso di applicabilità dell'**Ipotesi 3**, quale Responsabile Esterno del trattamento per quanto concerne la gestione di dati personali in titolarità del Committente, nonché quale Altro Responsabile con riferimento la gestione di dati personali in titolarità di altre Entità del Gruppo Iren.

Nell'esecuzione delle attività inerenti l'Incarico, il Fornitore s'impegna a porre in essere quanto segue:

1) assicurare che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza ed all'identità personale;
2) procedere al trattamento dei dati personali nel pieno rispetto delle Norme in materia di Protezione dei Dati Personali, in particolare per quanto riguarda la base giuridica necessaria per ciascun trattamento; ogni eventuale trasferimento dei dati personali verso un Paese terzo o un'organizzazione internazionale potrà avvenire solo ed esclusivamente per le finalità e secondo le modalità operative indicate da IREN nonché nel rispetto di quanto previsto dal GDPR con riguardo al trasferimento verso Paesi terzi;
3) i dati personali, contenuti nei database forniti da IREN, nella titolarità di IREN ovvero di una delle Entità legali appartenenti al Gruppo IREN indicate nell'Allegato B, devono essere utilizzati solo ed esclusivamente al fine di eseguire le attività inerenti l'Incarico. Di tali dati personali potrà essere fatta una copia a fini esclusivi di svolgimento delle attività connesse all'incarico ovvero per back–up, ed è espressamente vietato qualsiasi altro utilizzo, comunicazione, copia (parziale o totale) dei dati stessi senza il preventivo consenso scritto di IREN;
4) il trattamento od i trattamenti effettuati dal Fornitore consisteranno solo ed esclusivamente nelle operazioni necessarie per l'esecuzione dei propri obblighi previsti nel Contratto secondo quanto previsto dall'Incarico. Il fornitore si impegna ad evitare usi impropri (dolosi e colposi), anche da parte di dipendenti e collaboratori, dei dati la cui titolarità è di IREN;
5) nessun nuovo trattamento relativamente a tali dati può essere iniziato se non previa espressa comunicazione scritta in merito da parte di IREN;
6) il Fornitore s'impegna a rispettare tutte le indicazioni ricevute da IREN, di tempo in tempo, nonché ad adottare ogni ulteriore misura che, in relazione alle attività di cui all'Incarico, sia necessaria al fine garantire il pieno rispetto delle Norme in materia di Protezione dei Dati Personali;
7) il Fornitore ha individuato nominativamente, nell'ambito della propria struttura aziendale le persone che sotto la propria autorità sono autorizzate al trattamento e deve loro impartire le istruzioni necessarie, anche con riferimento agli obblighi di riservatezza e all'adozione e all'importanza delle misure tecniche e organizzative adeguate al livello di rischio, conformemente alle Norme in materia di Protezione dei Dati Personali. L'elenco di tali persone dovrà essere sempre disponibile e dovrà essere fornito immediatamente a IREN, su semplice richiesta di quest'ultima;
8) ove risulti necessario per l'esecuzione di specifiche attività di trattamento di cui al presente atto di nomina, il Fornitore è autorizzato a ricorrere ad altro Responsabile Esterno del trattamento (di seguito "**Altro Responsabile**"). L'elenco aggiornato degli Altri Responsabili viene fornito al Titolare del trattamento contestualmente alla sottoscrizione del presente atto di nomina. In caso di variazioni, il Responsabile comunicherà preventivamente le possibili modifiche al Titolare.

   Resta in ogni caso inteso che, ove l'Altro Responsabile individuato debba ricorrere ad un ulteriore Responsabile (di seguito "**Ulteriore Responsabile**") per l'esecuzione di determinate attività o porzioni di attività di trattamento, tale ulteriore trasferimento sarà legittimo solo previa espressa comunicazione da parte del Fornitore ed autorizzazione da parte del Committente.

   Il Fornitore verifica che gli Altri Responsabili rispettino le istruzioni, gli obblighi e le misure tecniche di

sicurezza necessarie in relazione alle specifiche attività di trattamento poste in essere. A semplice richiesta di IREN, il Fornitore metterà a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi in capo a ciascun Altro Responsabile.

9) Nel caso di variazione dell'elenco degli Altri Responsabili del trattamento ovvero di necessità di ricorso ad un aggiuntivo Altro Responsabile, ai sensi di quanto previsto dal paragrafo precedente:
   - Il Fornitore verifica che ogni Altro Responsabile individuato rispetti le istruzioni, gli obblighi e le misure tecniche di sicurezza necessarie in relazione alle specifiche attività di trattamento poste in essere. A semplice richiesta di IREN, il Fornitore metterà a disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi in capo a ciascun ulteriore responsabile;
   - IREN potrà opporsi all'attribuzione del ruolo di Altro Responsabile entro 10 (dieci) giorni lavorativi dopo la ricezione della comunicazione di richiesta di modifica della lista degli Altri Responsabili. In tal caso, il Fornitore farà ogni ragionevole sforzo per accogliere le richieste di IREN in modo da evitare il trattamento dei dati personali da parte dell'Altro Responsabile oggetto di opposizione, senza gravare irragionevolmente IREN;
   - Nell'eventualità che il Fornitore non possa rendere disponibile tale modifica entro un ragionevole periodo di tempo, che non deve eccedere 30 (trenta) giorni, IREN potrà recedere dal Contratto con riferimento alle sole attività che non possano essere fornite dal Fornitore senza l'utilizzo dell'Altro Responsabile oggetto di opposizione, mediante una comunicazione scritta. Il Fornitore rimborserà a IREN gli eventuali importi prepagati per le attività per cui sia stato esercitato il recesso, avuto riguardo alla durata del Contratto che residua dopo la data di efficacia del recesso, senza imporre alcuna penale in conseguenza a tale recesso;

   Resta inteso che, ai sensi di quanto previsto dall'art. 28 del GDPR, il Fornitore risponderà integralmente verso IREN di qualunque conseguenza derivante dal ricorso ad ogni Altro Responsabile del trattamento, tenendo IREN indenne da ogni conseguenza dannosa o pregiudizievole derivante dall'opera di ogni Altro Responsabile di cui il Fornitore si avvalga.

10) nella misura in cui il Fornitore decida di esternalizzare una parte delle attività di trattamento di cui al presente Atto di nomina avvalendosi di Altri e/o Ulteriori Responsabili stabiliti al di fuori dello Spazio Economico Europeo ("SEE"), ai sensi dell'articolo 46 par. 2 lett. c) del GDPR, il Fornitore e l'Altro e/o Ulteriore responsabile hanno stabilito Clausole contrattuali tipo ex DEC 2021/914/UE (anche "Clausole Contrattuali Standard" o "CCS") della Commissione Europea.

    Tanto precisato, ove necessario per ragioni di natura tecnica e/o operativa legate alle attività di supporto relative al servizio reso disciplinato nel Contratto, il Fornitore potrà trasferire – direttamente o a mezzo di Altri Responsabili – i dati personali in un Paese terzo per il quale la Commissione Europea abbia emesso un giudizio di adeguatezza del livello di protezione dei dati personali.

    In assenza di decisione di adeguatezza della Commissione Europea, il trasferimento dei dati personali è possibile solo in presenza di almeno una delle condizioni previste dal Capo V (articoli 44 e seguenti GDPR), ad esempio:

    - i trasferimenti di dati personali – nei limiti delle ragioni di natura tecnica e/o operativa legate alle attività di supporto relative al servizio reso - saranno possibili solo qualora il Fornitore fornisca adeguate garanzie di natura contrattuale, previa adeguata e documentata verifica, e si impegni a rispettare ed elaborare i dati personali in conformità a quanto previsto dalle Clausole Contrattuali Standard applicabili al trasferimento di dati da Titolare del trattamento a Responsabile del trattamento che dovranno essere - previo trasferimento - compilate, accettate, sottoscritte dal Fornitore e rese disponibili al Titolare;
    - i trasferimenti di dati personali – nei limiti delle ragioni di natura tecnica e/o operativa legate

alle attività di supporto relative al servizio reso – saranno possibili tra il Fornitore e Altri Responsabili - , solo qualora il Fornitore si impegni ad ottenere dal proprio Altro Responsabile adeguate garanzie di natura contrattuale e l'impegno di quest'ultimo a rispettare ed elaborare i dati personali in conformità alle Clausole Contrattuali Standard applicabili al trasferimento di dati da Responsabile del trattamento a Altro Responsabile del trattamento, che dovranno essere previamente compilate, accettate e sottoscritte dall'Altro Responsabile e rese disponibili al Titolare, qualora dallo stesso richieste.

11) il Fornitore dovrà effettuare i controlli necessari per accertare che i dati personali siano trattati dal proprio personale, nonché da ogni ulteriore responsabile del trattamento di cui all'art. 8 e 9 precedente, in modo lecito, raccolti, registrati e trattati per gli scopi determinati dall'Incarico, espliciti e legittimi, ed utilizzati con finalità e modalità conformi a quelle per le quali sono stati raccolti;
12) i dati personali relativamente ai quali ha valore il presente atto di nomina devono essere resi disponibili ed oggetto di trattamento solo ai dipendenti e/o collaboratori del che, per le loro mansioni, ne abbiano necessità in relazione all'esecuzione delle attività di cui all'Incarico e che siano stati debitamente incaricati del trattamento, ricevendo le istruzioni scritte previste per legge. I dati personali resi disponibili da IREN nell'ambito dell'Incarico non potranno essere resi disponibili o conosciuti da alcuna altra persona, fuori dagli Incaricati individuati dal Fornitore;
13) con riferimento alle attività di trattamento oggetto del presente atto, i dipendenti e collaboratori autorizzati al trattamento dei dati da parte del Fornitore, adibiti ai trattamenti di dati personali necessari per lo svolgimento dell'Incarico, agiranno sotto la supervisione e controllo del Fornitore, sollevando IREN da qualsiasi responsabilità per il loro operato;
14) i soggetti autorizzati al trattamento dei dati dovranno avere accesso solo ai dati personali necessari all'esecuzione delle loro mansioni e attività legate allo svolgimento dell'Incarico. È fatto espresso divieto per questi ultimi di porre in essere una qualsivoglia azione dolosa e colposa lesiva nei riguardi degli interessati;
15) il Fornitore dovrà tenere un registro delle attività di trattamento e renderlo disponibile ad IREN nonché alle autorità di controllo, ai sensi dell'art. 30 del GDPR;
16) il Fornitore metterà immediatamente a disposizione di IREN, su semplice richiesta di quest'ultima, tutto il supporto, tutti i dati e le informazioni ritenute ragionevolmente necessarie da IREN per consentire a quest'ultima di garantire agli interessati l'effettivo esercizio dei diritti previsti dagli artt.15-22 del GDPR; resta inteso tra le Parti che tutte le attività del Fornitore, ai sensi del presente paragrafo, sono comprese nei corrispettivi previsti per l'esecuzione dell'Incarico, fatta eccezione per eventuali richieste ulteriori da parte di IREN, nel qual caso le Parti concorderanno di volta in volta in forma scritta ed in buona fede;
17) il Fornitore non avrà alcun rapporto diretto con gli interessati i cui dati saranno trattati dal Fornitore medesimo. Tali dati personali saranno trattati dal Fornitore esclusivamente ai fini dell'esecuzione dell'Incarico. Il Fornitore riceverà i dati personali da trattare esclusivamente da IREN ovvero direttamente dalle Entità del Gruppo IREN indicate nell'Allegato B o da soggetti terzi specificatamente indicati per iscritto da IREN. Tuttavia, in caso di richieste di informazioni relativamente al trattamento dei dati od all'esercizio dei diritti previsti dagli artt.15-22 del GDPR che pervengano direttamente al Fornitore, questi si impegna a darne immediata notizia a IREN, concordando preventivamente le misure da adottare. IREN si riserva in ogni caso il diritto di rivalersi dei danni subiti nonché di ogni eventuale ulteriore conseguenza dannosa quale conseguenza della mancata comunicazione tempestiva da parte del Fornitore a IREN della richiesta pervenuta da un interessato;
18) il Fornitore si impegna a valutare l'adeguato livello di sicurezza in relazione ai rischi presentati dal trattamento dei dati oggetto del presente atto di nomina e alla luce di tale valutazione si impegna, per sé e per ogni eventuale Altro e/o Ulteriore Responsabile del trattamento di cui si avvale ai sensi degli artt. 8 e 9 precedenti, a predisporre tutte le misure di sicurezza necessarie e adeguate ai sensi dell'art. 32 del GDPR e del Decreto Legislativo 30 giugno 2003, n. 196 così come novellato dal Decreto Legislativo 10 agosto 2018, n. 101 - al fine di evitare rischi di perdita, distruzione o

manomissione, divulgazione non autorizzata o acceso in modo accidentale o illegale ai dati personali – di cui all'Allegato A al presente atto di attribuzione del ruolo;

19) il Fornitore è tenuto a notificare a IREN, senza ingiustificato ritardo dall'accertamento, eventuali violazioni della sicurezza dei dati personali trattati nell'ambito dell'Incarico (di seguito, "Violazione della Sicurezza") effettive o ragionevolmente sospette subite da parte del Fornitore o da parte di uno dei suoi ulteriori responsabili ai sensi degli artt. 8 e 9 precedenti.

    Il Responsabile Esterno, ove necessario, si impegna a informare il Titolare ai seguenti indirizzi:

    - DPO: dpo@gruppoiren.it
    - Ufficio Privacy: privacy.irenspa@gruppoiren.it
    - Indirizzo PEC: irenspa@pec.gruppoiren.it

20) il Fornitore fornirà tutta l'assistenza necessaria al fine di consentire a IREN la gestione della Violazione di Sicurezza. A questo scopo, il Fornitore fornisce a IREN, per ciascuna Violazione di Sicurezza, almeno le seguenti informazioni di dettaglio:
    - la descrizione della la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di record dei dati personali interessati;
    - la descrizione delle probabili conseguenze della violazione dei dati personali subite dal Fornitore e/o dagli ulteriori responsabili di cui agli art. 8 e 9 precedenti;
    - le misure adottate o da adottare per affrontare la violazione dei dati personali, per attenuare gli effetti e ridurre al minimo i danni derivanti dalla Violazione della sicurezza;
21) il Fornitore porrà in essere con i propri dipendenti e/o collaboratori o terzi fornitori tutti gli adempimenti formali e sostanziali (es. formazione) volti a garantire il rispetto delle Norme in materia di Protezione dei Dati;
22) il Fornitore dovrà dare piena collaborazione al Garante ed alle autorità pubbliche in caso di loro richieste di informazioni o di effettuazione di controlli, accessi ed ispezioni in relazione alle attività di cui all'Incarico e relativamente ai trattamenti affidatile con il presente atto di attribuzione del ruolo. Al riguardo darà pronta comunicazione ad IREN ed agirà esclusivamente previa consultazione di IREN e nell'ambito delle istruzioni ricevute da IREN. Ogni risposta al Garante o altra autorità dovrà essere preventivamente autorizzata da IREN;
23) in generale, sarà compito del Fornitore fare o suggerire quanto opportuno per l'attuazione delle presenti istruzioni ed in funzione del ruolo del Fornitore, tra l'altro riportando prontamente per iscritto qualunque evento od elemento che possa essere rilevante in relazione alle attività di cui all'Incarico, ed in particolare in relazione alla sicurezza dei dati;
24) il Fornitore infine si impegna ad impartire ai soggetti autorizzati al trattamento istruzioni in merito alle operazioni di trattamento ed a vigilare sulla loro puntuale applicazione;
25) *il* Fornitore*, ove necessario, procederà all'individuazione e nomina degli incaricati che operino quali Amministratori di Sistema, ai sensi del Provvedimento del Garante del 27 novembre 2008 in materia di Amministratori di Sistema, impartendo le relative istruzioni e vigilando, anche tramite verifiche periodiche (da eseguirsi almeno con cadenza annuale), sulla puntuale osservanza delle disposizioni ed istruzioni impartite, nonché provvedendo, in relazione ad esigenze occasionali e contingenti o a seguito di avvicendamenti, turnazioni o sostituzioni, agli adempimenti relativi nel rispetto delle norme di legge;*

    In particolare, il Fornitore si dovrà inoltre attenere alle seguenti istruzioni con riguardo agli Amministratori di Sistema:

    - *conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;*
    - *svolgere un'attività di verifica, con cadenza almeno annuale, sull'operato degli amministratori di sistema;*
    - *adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le*

registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Il Fornitore dichiara di aver esaminato e compreso le istruzioni sopra riportate e di essere competente per la piena attuazione di quanto ivi disposto.

Il Fornitore autorizza sin d'ora IREN ad intraprendere tutte le verifiche che si rendano necessarie circa la puntuale esecuzione degli obblighi derivanti dal presente atto di attribuzione del ruolo; IREN potrà condurre tali verifiche anche coinvolgendo altro soggetto da questi incaricato.

Tali verifiche, che potranno anche comportare l'accesso a locali o macchine e programmi del Fornitore, potranno aver luogo in seguito a comunicazione scritta da parte di IREN che sarà inviata con cinque giorni lavorativi di preavviso. Nell'ambito di tali verifiche, il Fornitore fornirà l'assistenza ed il supporto necessario, rispondendo alle richieste di IREN in relazione ai dati ed ai trattamenti in relazione ai quali ha valore il presente atto di attribuzione del ruolo.

Ai sensi dell'art. 82 GDPR, la responsabilità delle Parti, nonché di eventuali Altri e/o Ulteriori Responsabili di cui eventualmente si avvalga il Fornitore ai sensi dei precedenti artt. 8 e 9, è solidale per qualsiasi danno cagionato nei confronti degli Interessati nell'esecuzione delle attività di trattamento descritte nel presente Atto di Nomina. La Parte che abbia risarcito il danno per intero avrà diritto di rivalsa nei confronti dell'altra per la parte di risarcimento corrispondente alla propria responsabilità nella causazione del danno.

In caso di violazioni accertate dall'Autorità di controllo competente, ciascuna Parte sarà tenuta al pagamento dell'ammontare della sanzione contestata nei limiti della responsabilità rilevata a proprio carico dall'autorità di controllo.

Fatti salvi i casi di dolo o colpa grave, le eventuali ulteriori responsabilità del Fornitore per qualsiasi altro danno che potrebbe derivare nei confronti di IREN a seguito di una violazione imputabile al Fornitore medesimo o agli eventuali Altri e/o Ulteriori Responsabili di cui eventualmente si avvale (i) degli obblighi imposti dalla Legge Applicabile e/o (ii) delle istruzioni di cui al presente Atto di Nomina, è disciplinata dalle disposizioni in tema di responsabilità contrattuale delle Parti di cui al Contratto stipulato.

Resta inteso che il presente atto di attribuzione del ruolo di responsabile del trattamento ha valore fino alla conclusione dello svolgimento delle attività richieste dall'Incarico, di cui al Contratto, e che al termine delle stesse ogni dato personale fornito nell'ambito delle attività di cui all'Incarico dovrà essere restituito a IREN ovvero distrutto, secondo le modalità operative che verranno indicate da IREN al momento.

Allegato A
MISURE DI SICUREZZA INDIVIDUATE PER LIVELLO DI RISCHIO

Allegato A
ISTRUZIONI DI SICUREZZA

Allegato contenente le istruzioni di sicurezza – MEDIO rischio

Allegato A della Lettera di Nomina a Responsabile (o sub-responsabile) Esterno

Requisiti di sicurezza

Il Responsabile Esterno garantisce il possesso dei requisiti di sicurezza dettagliati nel presente Allegato per l'intera durata del trattamento dei dati.
I requisiti di sicurezza richiesti al Responsabile Esterno sono riportati:

- Nella **Sezione 1** nel caso in cui il Responsabile Esterno acceda solamente ai dati personali di cui il Committente e/o le altre società del Gruppo Iren sono Titolari, senza che questi siano memorizzati su dispositivi/infrastruttura non di proprietà del Gruppo Iren;

- Nella **Sezione 2** nel caso in cui i dati personali di cui il Committente e/o le altre società del Gruppo Iren sono Titolari siano trasferiti su dispositivi/infrastruttura del Responsabile Esterno (ad titolo esemplificativo: su workstation, DB, ambienti di sviluppo/test/produzione gestiti dal Responsabile Esterno).

Il Responsabile Esterno garantisce inoltre:

- l'applicazione e il rispetto dei Principi previsti dal Regolamento UE 2016/679 (GDPR), quali il Principio di Privacy by Design, il Principio di Minimizzazione dei dati trattati e il Principio di Limitazione della conservazione. In applicazione del Principio di Limitazione della conservazione, il Responsabile Esterno si impegna a rispettare e, ove necessario, implementare il periodo di conservazione dei dati personali definito dal Gruppo Iren o previsto da obblighi di legge a cui il Responsabile o il Titolare sono soggetti;
- di essere in grado di identificare sui suoi archivi fisici o virtuali in modo puntuale i dati personali che tratta per conto del Gruppo Iren al fine di poter rispondere ai requisiti regolamentari quali il rispetto della data retention, l'esercizio dei diritti degli interessati, la segnalazione di possibili violazioni di dati personali.

Sezione 1.

	Il Responsabile Esterno garantisce:
Politiche e procedure per la protezione e la gestione dei dati personali	➢ L'esistenza di politiche di sicurezza e di procedure operative specifiche relative alla sicurezza dei dati personali (quali, ad esempio: policy per la gestione dei diritti degli interessati, gestione dei data breach): - che prevedono la chiara distinzione di ruoli e responsabilità in materia di protezione dati personali; - adeguatamente inventariate; - opportunamente documentate ed adeguatamente riviste e aggiornate; - approvate dalle Direzioni e/o Responsabili; - comunicate adeguatamente a tutto personale interno ed esterno che verrà in contatto con i dati personali relativi al Gruppo IREN.
Ruoli e responsabilità	➢ La definizione e assegnazione dei ruoli e delle responsabilità relative al trattamento dei dati personali, coerentemente con quanto definito all'interno della politica di sicurezza adottata (di cui alla sezione precedente). ➢ La nomina delle persone incaricate della gestione della sicurezza dei dati personali.
Politica di gestione degli accessi	➢ [*Qualora la definizione degli accessi ai sistemi sia in capo al Responsabile Esterno*] Nell'ambito della gestione degli accessi ai sistemi che contengono dati personali, l'esistenza di una politica di gestione degli accessi formalizzata che preveda: - il rispetto del principio del Need to Know, in modo tale che l'accesso ai dati personali sia riservato al solo personale che ne ha reale necessità (ad esempio: restrizioni in base ai ruoli).
Responsabile Esterno del Trattamento	[*Qualora il Responsabile Esterno:* *- si avvalga (anche in parte) di un sub-fornitore/processor nell'esecuzione delle attività inerenti i trattamenti*

	di dati di cui il Gruppo è Titolare; *- abbia un Titolare del trattamento diverso da quello del sub-fornitore/processor di cui al punto precedente (es. il subfornitore non sia una società controllata/collegata del Responsabile Esterno)*] ➢ Ai sub-fornitori/processor vengono richiesti gli stessi requisiti identificati nel presente Allegato.
Gestione degli incidenti/ Violazione dei dati personali	➢ L'esistenza di una procedura di gestione degli incidenti/violazioni relative ai dati personali. - Qualora si verifichi una violazione di dati personali (data breach), la procedura contempla un processo di notifica alle Autorità competenti, agli interessati e al Titolare .
Riservatezza del personale e Formazione	➢ L'adeguata informazione e formazione nei confronti dei dipendenti in merito alle proprie responsabilità, agli obblighi relativi al trattamento dei dati personali e alla politica di sicurezza dell'organizzazione (prima che inizino a trattare i dati personali del Titolare).
Controllo degli accessi e autenticazione	In merito al controllo degli accessi e all'autenticazione delle risorse IT utilizzate per accedere ai sistemi su cui sono presenti dati personali: ➢ L'esistenza di un sistema di controllo degli accessi alle risorse IT, che consenta la gestione dei processi di creazione, revisione e cancellazione degli account utente. ➢ L'uso di account condivisi opportunamente limitato ai soli casi in cui strettamente necessario. ➢ L'esistenza di una password policy formalmente documentata che identifichi i principali requisiti di complessità e di aggiornamento delle password degli utenti e che rispetti almeno i seguenti requisiti: - complessità password: minimo 8 caratteri (tra cui almeno 3 tra i seguenti tipi di caratteri: maiuscola, minuscola, numeri, caratteri speciali); - cambio password obbligatorio dopo il primo utilizzo; - periodo di validità password: massimo 90 giorni; - credenziali disabilitate massimo dopo 90 giorni di inattività. ➢ L'utilizzo di tecniche di mascheramento delle password degli utenti (ad es. mediante funzione di "hash").
Sicurezza della workstation	➢ Workstation utilizzate per il trattamento di dati personali: - aventi impostazioni di sicurezza non bypassabili da parte degli utenti; - su cui sono installate le principali misure di sicurezza (es. antivirus, firme di rilevamento, sessioni limitate, aggiornamenti critici di sicurezza). Tali misure di protezione sono costantemente aggiornate.
Rete/sicurezza della comunicazione	➢ La limitazione dell'accesso alle risorse aziendali da remoto o mediante rete wireless ai soli casi in cui è strettamente necessario. ➢ L'accesso ai sistemi, se effettuato da remoto (via internet), avviene utilizzando protocolli di comunicazione sicuri (es.SSL).
Mobile/dispositivi portatili	*[Qualora sia possibile accedere ai dati personali di cui il Gruppo è Titolare anche mediante dispositivi portatili le cui configurazioni di sicurezza siano definite dal Responsabile Esterno]* - la protezione dell'accesso al dispositivo mediante password o pin obbligatori; - la formale definizione dei ruoli e delle responsabilità per la gestione dei dispositivi mobili.
Trasparenza e tutela dei diritti	➢ Adeguato supporto al Titolare nell'evasione delle istanze relative sia alle richieste di esercizio dei diritti da parte di un interessato (accesso, rettifica, cancellazione/oblio, opposizione, portabilità, limitazione) sia informazioni sui responsabili esterni.

Sezione 2.

	Il Responsabile Esterno garantisce:
Politiche e procedure per la protezione e la gestione dei dati personali	➢ L'esistenza di politiche di sicurezza e di procedure operative specifiche relative alla sicurezza dei dati personali (quali, ad esempio: policy per la gestione dei diritti degli interessati, gestione dei data breach): - che prevedono la chiara distinzione di ruoli e responsabilità in materia di protezione dati personali; - adeguatamente inventariate; - opportunamente documentate ed adeguatamente riviste e aggiornate; - approvate dalle Direzioni e/o Responsabili; - comunicate adeguatamente a tutto personale interno ed esterno che verrà in contatto con i dati personali relativi al Gruppo Iren. ➢ L'esistenza di attività di audit periodici sui sistemi informativi aziendali che gestiscono i dati personali trattati per conto del Titolare, al fine di verificarne la conformità con le politiche e gli standard di sicurezza adottati (di cui al punto precedente).
Ruoli e responsabilità	➢ La definizione e assegnazione dei ruoli e delle responsabilità relative al trattamento dei dati personali, coerentemente con quanto definito all'interno della politica di sicurezza adottata (di cui alla sezione precedente). ➢ La nomina delle persone incaricate della gestione della sicurezza dei dati personali.
Politica di gestione degli accessi	➢ L'esistenza di una politica di gestione degli accessi ai dati personali, adeguatamente formalizzata, che preveda specifiche regole di controllo degli accessi in base al principio del Need to Know, ovvero che garantisca che l'accesso ai dati sia riservato al solo personale che ne ha reale necessità (ad esempio: restrizioni per ruoli specifici degli utenti). - Nell'ambito della gestione degli accessi ai sistemi che gestiscono dati personali, è definita e documentata la segregazione dei ruoli e delle responsabilità (ad esempio: Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi).
Risorse/gestione delle risorse	➢ L'esistenza di un registro delle risorse IT (hardware, software e rete) utilizzate per il trattamento dei dati personali, regolarmente aggiornato. ➢ La definizione dei ruoli aziendali che hanno accesso alle risorse IT utilizzate per il trattamento dei dati personali.
Change Management	➢ In ambito di Change Management, l'esistenza di un ambiente dedicato allo sviluppo/ test delle modifiche applicative, segregato da quello di produzione e non contenente dati reali. - Ove l'utilizzo di dati fittizi non fosse tecnicamente consentito, sono formalmente identificate le misure tecniche in essere per limitare l'accesso ai dati personali presenti in ambiente di test al solo personale autorizzato.
Responsabile Esterno del Trattamento	[*Qualora il Responsabile Esterno:* *- si avvalga (anche in parte) di un sub-fornitore/processor nell'esecuzione delle attività inerenti i trattamenti di dati di cui il Gruppo è Titolare;* *- abbia un Titolare del trattamento diverso da quello del sub-fornitore/processor di cui al punto precedente (es. il subfornitore non sia una società controllata/collegata del Responsabile Esterno)*] ➢ Ai sub-fornitori/processor vengono richiesti gli stessi requisiti identificati nel presente Allegato.
Gestione degli incidenti/ Violazione dei dati personali	➢ L'esistenza di una procedura di gestione degli incidenti/violazioni relative ai dati personali. - Qualora si verifichi una violazione di dati personali (data breach), la procedura contempla un processo di notifica alle Autorità competenti, agli interessati e al Titolare.
Business continuity	➢ L'esistenza di un piano di business continuity dettagliato (con chiara definizione dei ruoli e delle responsabilità e del livello di qualità del servizio garantito), documentato e adeguato per garantire il livello richiesto di continuità e disponibilità dei sistemi che elaborano i dati personali (in caso di incidente / violazione dei dati personali).
Riservatezza del personale e Formazione	➢ L'adeguata informazione e formazione nei confronti dei dipendenti in merito alle proprie responsabilità, agli obblighi relativi al trattamento dei dati personali e alla politica di sicurezza dell'organizzazione (prima che inizino a trattare i dati personali del Titolare).

Controllo degli accessi e autenticazione	[*Qualora la definizione dei requisiti di autenticazione (si veda sotto) ai sistemi contenti dati personali di cui il Gruppo è Titolare sia in capo al Responsabile Esterno*] ➢ L'esistenza di un sistema di controllo degli accessi alle risorse IT, che consenta la gestione dei processi di creazione, revisione e cancellazione degli account utente. ➢ L'uso di account condivisi opportunamente limitato ai soli casi in cui strettamente necessario. ➢ L'esistenza di una password policy formalmente documentata che identifichi i principali requisiti di complessità e di aggiornamento delle password degli utenti e che rispetti almeno i seguenti requisiti: - complessità password: minimo 8 caratteri (tra cui almeno 3 tra i seguenti tipi di caratteri: maiuscola, minuscola, numeri, caratteri speciali); - cambio password obbligatorio dopo il primo utilizzo; - periodo di validità password: massimo 90 giorni; - credenziali disabilitate dopo massimo 90 giorni di inattività. ➢ L'utilizzo di tecniche di mascheramento delle password degli utenti (ad es. mediante funzione di "hash").
Log e monitoraggio	[*Qualora il responsabile esterno abbia accesso ai log degli applicativi o dei sistemi contenenti dati personali di cui il Gruppo è Titolare*] ➢ La registrazione e il monitoraggio dei log per tutti gli applicativi e i sistemi coinvolti nel trattamento dei dati personali per tracciare tutte le attività degli Amministratori di Sistema (log in, log out e tutte le azioni di modica, cancellazione e visualizzazione). ➢ La protezione adeguata dei file di log contro manomissioni e accessi non autorizzati.
Server/sicurezza dei database	➢ La gestione dei server dei database tramite account dedicati e con limitati diritti di accesso. ➢ L'adozione di soluzioni di crittografia e/o psudoanonimizzazione sui dati personali, in accordo ad una policy formalmente definita.
Sicurezza della workstation	[*Qualora il Responsabile Esterno abbia accesso ai dati personali di cui il Gruppo è Titolare mediante workstation di cui definisca le configurazioni di sicurezza*] ➢ Workstation utilizzate per il trattamento di dati personali: - aventi impostazioni di sicurezza non bypassabili da parte degli utenti; - su cui sono installate le principali misure di sicurezza (es. antivirus, firme di rilevamento, sessioni limitate, aggiornamenti critici di sicurezza). Tali misure di protezione sono costantemente aggiornate.
Rete/sicurezza della comunicazione	[*Qualora la definizione delle configurazioni di sicurezza per l'accesso da remoto ai sistemi contenenti dai personali di cui il Gruppo è Titolare sia in capo al Responsabile Esterno*] ➢ La limitazione dell'accesso alle risorse aziendali da remoto o mediante rete wireless ai soli casi in cui è strettamente necessario. ➢ La gestione dell'accesso via internet alle risorse aziendali mediante l'utilizzo di protocolli di comunicazione sicuri (es.SSL). ➢ L'accesso via internet adeguatamente monitorato da personale identificato (es. responsabile della sicurezza) e limitato mediante l'utilizzo di misure tecniche adeguate (es. firewall, IPS, etc.).
Back-up	➢ L'esecuzione regolare e adeguatamente monitorata di back-up completi dei dati personali trattati. ➢ Le copie dei dati sono oggetto di un livello di protezione coerente con quanto applicato sui dati di origine e archiviate in un luogo distinto da quello di archiviazione dei dati di origine. ➢ L'esecuzione di Test di restore periodici.
Mobile/dispositivi portatili	*[Qualora sia possibile accedere ai dati personali di cui il Gruppo è Titolare anche mediante dispositivi portatili le cui configurazioni di sicurezza siano definite dal Responsabile Esterno]* - la protezione dell'accesso al dispositivo mediante password o pin obbligatori; - la formale definizione dei ruoli e delle responsabilità per la gestione dei dispositivi mobili.
Sicurezza del ciclo di vita delle applicazioni	➢ Durante la fase di sviluppo delle applicazioni che trattano dati personali, è prevista una fase di test dei requisiti di sicurezza stabiliti in fase di progettazione. ➢ L'esecuzione periodica di test di vulnerabilità e penetration test da parte di una terza parte accreditata. ➢ Le patch software sono testate in ambiente di test prima di essere trasportate in produzione.
Cancellazione dei dati/dismissione	➢ La sovrascrittura di tutti i dispositivi contenenti dati personali o, in alternativa, la loro distruzione fisica. ➢ La cancellazione periodica dei file temporanei.
Sicurezza fisica	➢ La protezione del perimetro fisico dell'infrastruttura del sistema IT da accessi non autorizzati tramite sistema di rilevamento intrusioni o barriere fisiche. ➢ Il monitoraggio degli accessi ai locali dell'organizzazione sia da parte del personale interno che dei visitatori (ad esempio tramite lettori badge identificativi).

	➢ La registrazione (registro fisico o registrazione a traccia elettronica) di tutti gli accessi alle zone sicure (es. sala server). - Tali accessi sono limitati al solo personale autorizzato. ➢ La protezione della sala server mediante un sistema antincendio automatico, un sistema di climatizzazione dedicato a controllo chiuso e un gruppo di continuità (UPS).
Trasparenza e tutela dei diritti	➢ Ove applicabile, la comunicazione agli interessati circa il trattamento dei loro dati personali avviene: - prima di implementare il trattamento; - tramite informativa facilmente accessibile e comprensibile; - ove applicabile, fornendo i mezzi necessari affinché gli interessati possano esercitare il proprio consenso specifico, libero, per ciascuna finalità, informato, inequivocabile e dimostrabile. ➢ Adeguato supporto al Titolare nell'evasione delle istanze relative alle richieste di esercizio dei diritti da parte di un interessato (accesso, rettifica, cancellazione/oblio, opposizione, portabilità, limitazione) sia informazioni sui responsabili esterni.