ALLEGATO B

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 28 del Regolamento UE 2016/679

Tra

EOLO SpA, con sede in Busto Arsizio (VA), via Gran San Bernardo n°12, C.F. e P. IVA n. 02487230126 ("***EOLO***" o la "***Società***" o il "***Titolare del Trattamento***" o il "***Titolare***"), in persona di Guido Maria Garrone, in qualità di Amministratore Delegato, munito dei necessari poteri,

e

[HQ ENGINEERING ITALIA SRL], con sede legale in [MILANO], via [GIORGIO STEPHENSON 29, 20157], P. IVA e CF n° [06997160962] (di seguito, il "***Fornitore***", il "***Responsabile del Trattamento***" o il "***Responsabile***"), in persona del suo legale rappresentate pro-tempore,

di seguito congiuntamente indicate come "**Parti**"

Premesso che:

a) EOLO è una società operante nel settore delle Telecomunicazioni;
b) Nell'esercizio della sua attività, la Società ha accesso e tratta i dati personali di diversi soggetti (gli "**Interessati**");
c) Ill Fornitore è una società specializzata nei servizi di consulenza professionale per la progettazione di postazioni radio idonee all'installazione di apparati di trasmissione per l'esercizio di servizi di telecomunicazione, compresa la ricerca e l'acquisizione dell'ospitalità presso i relativi siti (mediante la negoziazione di locazioni o altri contratti per il godimento di beni immobili);
d) La Società ha stipulato con il Fornitore un contratto denominato "CONTRATTO DI SERVIZI DI ACQUISIZIONE E PROGETTAZIONE SITI PER LA REALIZZAZIONE DI IMPIANTI DI TELECOMUNICAZIONE"
e dei Contenuti e Servizi ad essa collegati, come meglio definiti nel Contratto, il cui adempimento comporta, tra l'altro, che il Fornitore tratti dati personali per conto del Titolare ed è, quindi, soggetto alle previsioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati – "*GDPR*");
e) La Società, quale Titolare del Trattamento, ha determinato le finalità e i mezzi delle attività di trattamento dei predetti dati personali (i "**Dati Personali del Titolare**") come meglio descritti nella presente nomina a responsabile del trattamento;
f) l'art. 4.8) del GDPR definisce "*Responsabile del Trattamento*" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

g) l'art. 28 del GDPR prevede che (i) qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato; (ii) i trattamenti da parte di un responsabile del trattamento siano disciplinati da un contratto o da altro atto giuridico ai sensi del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento;
h) il Fornitore è risultato essere in possesso di idonei requisiti di esperienza, capacità tecnico-economica ed affidabilità e presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate ai sensi delle previsioni del GDPR in materia di protezione dei dati personali e diritti degli interessati;
i) Le Parti, pertanto, a seguito della stipulazione del Contratto e ai sensi dell'art. 28 del GDPR, intendono procedere, per mezzo del presente allegato al Contratto (l'"**Addendum**") a definire le modalità con cui il Responsabile del Trattamento si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei Dati Personali come di seguito definite.

Tutto ciò premesso, tra le Parti si conviene e stipula quanto segue

Articolo 1 – Premesse e Addendum

1.1. Le Premesse al presente Addendum formano parte integrante ed essenziale dello stesso.
1.2. L'Addendum forma parte integrante ed essenziale del Contratto. I termini utilizzati nell'Addendum avranno il significato attribuito loro nell'Addendum stesso. I termini con la lettera maiuscola non altrimenti definiti nell'Addendum avranno il significato loro ascritto nel Contratto.

Articolo 2 – Definizioni

2.1 Nell'Addendum i seguenti termini avranno il significato che segue:

"**Data Breach**": una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, secondo quanto previsto dall'art. 4 (12) del GDPR e il cui verificarsi comporta gli effetti e gli obblighi di cui all'art. 33 del GDPR.

"**Dati Personali del Titolare**" o "**Dati Personali"**: i dati personali come definiti dal GDPR che formano oggetto delle attività di trattamento da parte del Responsabile del Trattamento per conto del Titolare del Trattamento, ai sensi del e in connessione all'esecuzione del Contratto.

"DPIA": va inteso come data protection impact assessment, ovvero valutazione di impatto sulla protezione dei dati, come disciplinata dall'art. 35 del GDPR. Si tratta di una procedura finalizzata a descrivere le attività di trattamento di dati personali, valutarne necessità e proporzionalità e facilitare la gestione dei rischi che le stesse possono implicare per i diritti e le libertà delle persone fisiche (attraverso una valutazione di tali rischi e la individuazione delle misure idonee ad affrontarli).

"DPO": si intende il *data protection officer* o responsabile della protezione dei dati, ai sensi dell'art. 37 del GDPR.

"**GDPR**": il Regolamento Europeo n. 2016/679 sulla protezione dei dati personali.

"**Servizi**": i servizi e le altre attività che dovranno essere eseguiti dal Fornitore o per suo conto a favore del Titolare ai sensi del Contratto.

"**Legge Applicabile**": è da intendere come qualsiasi disposizione normativa dell'Unione Europea o dello Stato membro alla cui legge la Società è soggetta, in materia di protezione dei Dati Personali, ivi inclusi i provvedimenti adottati di tempo in tempo, in materia di protezione dei dati personali, dall'Autorità Garante Italiana per la Protezione dei Dati Personali e dal Comitato dei Garanti Europei.

"**Soggetto Collegato**": qualsiasi soggetto partecipato o controllato da una delle Parti, ovvero in cui una delle Parti detenga una partecipazione o su cui eserciti un controllo o che sia soggetto al comune controllo o partecipazione di una delle Parti, laddove la definizione di controllo dovrà intendersi quella di cui all'art. 2359 c.

"**Sub-Responsabile**": ciascun soggetto (incluso qualsiasi terzo e qualsiasi Soggetto Collegato al Fornitore ma esclusi i dipendenti del Fornitore o dei suoi sub-contractor) delegato dal Fornitore a effettuare alcune operazioni di trattamento per conto del Titolare in connessione con il Contratto.

"Clausole contrattuali standard" Si intendono le clausole contrattuali standard per il trasferimento di dati personali da un titolare del trattamento dei dati sito nello Spazio Economico Europeo a soggetti stabiliti in Paesi terzi, adottate dalla Commissione europea ai sensi della normativa applicabile.

I termini "**Titolare**", "**Responsabile**", "**Interessato**", "**Stato Membro**", "**dati personali**", "**Trattamento**" ed "**Autorità Garante**" avranno il significato loro ascritto nel GDPR e dovranno essere interpretati di conseguenza.

Articolo 3 – Oggetto delle prestazioni del Responsabile del Trattamento

3.1. Il Responsabile del Trattamento è autorizzato a trattare per conto del Titolare del Trattamento i Dati Personali necessari per fornire i Servizi.

3.2. Dati Personali oggetto di trattamento sono comuni, quali dati anagrafici e dati di contatto.

3.3. La natura delle operazioni realizzate sui dati personali è sia automatizzata che non automatizzata.

3.4. Il trattamento è finalizzato all'erogazione della fornitura di cui in oggetto al Contratto.

3.5. Le categorie di interessati sono i dipendenti e fornitori di EOLO.

Articolo 4 – Obblighi del Responsabile del Trattamento

4.1 Ai sensi dell'art. 28, comma terzo, del GDPR, il Fornitore quale Responsabile del Trattamento (così come chiunque svolga operazioni di trattamento sotto le sue istruzioni) sarà tenuto all'osservanza dei seguenti obblighi.

a) ***Rispetto della normativa.*** Attenersi scrupolosamente a e rispettare, nel trattamento dei Dati Personali, la Legge Applicabile.

b) ***Rispetto delle finalità***. Trattare i Dati Personali esclusivamente per la finalità o le finalità specificate all'articolo 3 che precede e per l'esecuzione delle prestazioni dedotte nel Contratto, nonché conformemente alle istruzioni documentate in forma scritta da parte del Titolare. Il Responsabile del Trattamento dovrà, quindi, astenersi dal fare uso dei Dati Personali per finalità diverse da quelle specificate dal Titolare del Trattamento. I Dati Personali trattati dal Responsabile del Trattamento rimarranno di proprietà del Titolare e/o degli Interessati. Il Responsabile del Trattamento non dovrà assumere decisioni unilaterali concernenti le attività di trattamento per finalità diverse da quelle previste, ivi inclusa la decisione di comunicare tali dati a soggetti terzi e quella relativa ai tempi di conservazione dei Dati Personali del Titolare.

c) ***Dovere di cooperazione***. Informare immediatamente il Titolare (i) se ritenga che un'istruzione impartita dal Titolare del Trattamento comporti una violazione delle disposizioni del GDPR o, più in generale, della Legge Applicabile e (ii) dell'esistenza dell'obbligo giuridico di procedere ad un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, a meno che la normativa vigente vieti tale informazione per rilevanti motivi di interesse pubblico.

d) ***Riservatezza***. Garantire la riservatezza dei Dati Personali trattati e, in particolare, che (i) l'accesso ai Dati Personali sia limitato alle sole persone che hanno necessità di conoscere e/o accedere a tali dati per le finalità di cui al Contratto (i c.d. "**Soggetti Autorizzati al Trattamento**") e (ii) i Soggetti Autorizzati al trattamento dei Dati Personali si siano previamente impegnati alla riservatezza o siano, comunque, assoggettati ad un adeguato obbligo legale di riservatezza e abbiano ricevuto un'adeguata formazione in materia di protezione dei dati personali.

e) ***Sicurezza.*** Tenuto conto dello stato delle conoscenze tecniche, dei costi di realizzazione e della natura, della finalità, del contesto e dello scopo del trattamento nonché dei diversi livelli di rischio (in termini di gravità e probabilità) che il trattamento comporta per i diritti e le libertà fondamentali degli Interessati, adottare le misure di sicurezza tecnica e organizzativa adeguate ad assicurare un livello di sicurezza appropriato rispetto al rischio di perdita, alterazione o illegittimo trattamento dei Dati Personali gestiti per conto del Titolare, ivi incluse, ove applicabili, le misure di cui all'art. 32 (1) del GDPR. Nel valutare il livello di sicurezza appropriato in relazione al rischio, il Fornitore dovrà tenere in considerazione in particolare i rischi implicati dalle specifiche attività di trattamento dallo stesso compiute, ivi inclusi i rischi implicati dalla Violazione dei Dati Personali. In ogni caso il Responsabile del Trattamento dovrà garantire almeno l'adozione delle seguenti misure di sicurezza tecnica e organizzativa:
   - implementazione e gestione degli opportuni profili di accesso ai sistemi ed alle funzionalità applicative che consentono agli incaricati di gestire i dati personali dei clienti e, ove applicabili, funzionalità di cifratura delle informazioni presenti sull'HD dei laptop in uso al personale ed utilizzo di funzionalità di cifratura delle chiavette USB, al fine di assicurarne su base permanente riservatezza;
   - implementazione dei controlli di qualità necessari a validare le procedure operative in uso con riguardo anche alle procedure di gestione di eventuali documenti cartacei contenenti dati personali dei clienti ed altri controlli di qualità in ambito tecnologico atti a validare il software rilasciato in produzione, modo da garantirne l'integrità;

- utilizzo delle opportune procedure di backup insieme all'implementazione di eventuali architetture di alta affidabilità dei sistemi, atti a garantirne la disponibilità;
- implementazione ed aggiornamento di sistemi a protezione di dati ed applicazioni per far fronte a violazioni e attacchi mirati, azioni di pirateria, minacce del Web ed uso a distanza di vulnerabilità, atti a garantirne riservatezza, integrità e disponibilità.

In generale, si richiede al Fornitore di adottare tutte quelle misure tecniche ed organizzative che garantiscono un livello di sicurezza adatto al rischio, capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico e l'implementazione di procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. Si richiede inoltre al Fornitore la compilazione e la verifica di quanto previsto alla Sezione A4.

f) ***Amministratori di Sistema***: Atteso che gli Amministratori di Sistema (AdS) sono posti sotto la diretta autorità e il controllo del Responsabile, osservare le seguenti prescrizioni:
   i. aver adeguatamente individuato, istruito, informato, formato e designato tali amministratori, sulla base dell'esperienza, della capacità e affidabilità, con specifico atto scritto controfirmato, con le specifiche e i criteri dettati dalla relativa normativa;
   ii. implementare specifici e periodici corsi di formazione per gli AdS;
   iii. verificare periodicamente, e almeno una volta l'anno, l'attività degli AdS al fine di valutarne la conformità con le misure tecniche, organizzative e di sicurezza, secondo quanto previsto dalla norma;
   iv. predisporre adeguati standard di sicurezza idonei a garantire la rispondenza delle attività degli AdS alle misure richieste;
   v. conservare e fornire se richiesto con sollecitudine, e comunque entro 48 ore, il relativo elenco aggiornato completo degli AdS che trattano i dati personali di cui alla presente nomina;
   vi. ove i dati personali siano presenti sui sistemi informativi del Responsabile, adottare sistemi idonei alla registrazione degli accessi logici (cd. access log) ai sistemi garantendo che la registrazione abbia le caratteristiche richieste dal provvedimento del Garante sugli Amministratori di Sistema e dunque siano conservati per un congruo periodo, non inferiore a sei mesi;
   vii. in ogni caso attenersi scrupolosamente ai provvedimenti del Garante per la riservatezza, tra i quali il provvedimento del 27 novembre 2008, in tema di Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema, nonché, salvo preventiva autorizzazione scritta del Titolare, non trasferire i dati sui sistemi informativi di soggetti diversi dal Responsabile, anche in tecnologie cloud computing e similari.
   viii. Le relative anagrafiche degli AdS, ottenute per gli adempimenti richiesti dalla legge, saranno trasmesse dal Titolare a terzi legittimamente autorizzati.

Inoltre, per le attività svolte su sistemi del Titolare, il Responsabile nell'ambito della propria autonomia organizzativa si impegna a far osservare ai propri incaricati, che saranno da esso

nominati Amministratori di Sistema, le indicazioni conformi con quanto previsto nella Sezione A1 del presente Addendum.

g) ***Sub-Responsabili***: in virtù dell'autorizzazione generale da parte della Società a nominare altri soggetti come sub-responsabili, il Fornitore è tenuto ad informare periodicamente il Titolare in merito all'aggiunta o la sostituzione di altri responsabili del trattamento, fornendo descrizione dell'identità dei soggetti e dell'attività delegata, dando così al Titolare l'opportunità di opporsi a tali modifiche. inoltre, il Titolare conferisce espressamente mandato al Responsabile, ai sensi dell´art. 1704 c.c., al trasferimento dei Dati Personali del Titolare a Sub-Responsabili stabiliti presso Paesi non appartenenti allo Spazio Economico Europe ('SEE'), mediante la sottoscrizione delle Clausole Contrattuali Standard, di cui alla decisione della Commissione europea del 5 febbraio 2010, n. 87/2010/UE, ed approvate dal Garante con delibera del 27 maggio 2010, n. 35, oppure per mezzo delle specifiche garanzie adeguate previste all'art.46 del GDPR (es. EU-US Privacy Shield, BCR, etc.). Del contratto stipulato tra Responsabile e il relativo Sub-Responsabile, così come comprensivo delle ivi menzionate Clausole Contrattuali Standard (5 febbraio 2010, n. 87/2010/UE), o dell'utilizzo dell'ivi menzionate specifiche garanzie adeguate previste dal GDPR, verrà data opportuna evidenza al Titolare.

h) ***Trasferimento dei Dati Personali gestiti per conto del Titolare***. Il Responsabile del Trattamento potrà trattare i Dati Personali in paesi siti al di fuori dell'Unione Europea nonché trasferirli in tali paesi a condizione che i suddetti paesi garantiscano il livello di protezione dei dati e il rispetto degli altri obblighi previsti dalla normativa europea nonché da questo Addendum. Il Responsabile del Trattamento è tenuto ad informare il Titolare del Trattamento in merito ai paesi in cui i Dati Personali saranno trattati o trasferiti.

i) ***Diritti degli Interessati.*** Tenuto conto della natura del trattamento, assistere il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, 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 GDPR (il diritto di accesso, di rettifica, di cancellazione e di opposizione, alla limitazione del trattamento, alla portabilità dei dati, di non essere oggetto di una decisione individuale automatizzata). Nell'ipotesi in cui gli Interessati presentino richiesta per l'esercizio dei suddetti diritti al Responsabile del Trattamento, quest'ultimo dovrà inoltrare immediatamente, e comunque entro 72 ore dalla ricezione, detta richiesta per posta elettronica al Titolare del Trattamento, utilizzando l'indirizzo email *privacy@eolo.it*.

j) ***Cooperazione in caso di Data Breach e redazione di DPIA***. Assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR e, pertanto, nella elaborazione e nell'attuazione delle misure di sicurezza, nella notifica e nella comunicazione dei Data Breach, nella redazione della DPIA e nella consultazione preventiva, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del Trattamento.

   In particolare:

   - nel caso di Data Breach (violazione di dati personali), il Responsabile del Trattamento dovrà notificare al Titolare del Trattamento ogni potenziale violazione di dati personali riscontrata, a prescindere da qualsiasi valutazione circa l'impatto e le conseguenze attese

della violazione stessa, senza indugio e, in ogni caso, entro il tempo massimo di 48 ore dal momento in cui ne sia venuto a conoscenza utilizzando l'indirizzo email del DPO dpo@eolo.it corredando detta comunicazione con ogni documentazione utile a consentire al Titolare, quale Titolare del Trattamento, di notificare tale violazione al Garante e agli Interessati, ove necessario, nel rispetto delle tempistiche di cui all'art. 33 del GDPR. Tale sommaria comunicazione dovrà, in ogni caso, contenere quantomeno i seguenti dettagli: (i) l'indicazione della probabile causa della violazione; (ii) le conseguenze note o attese di tale violazione; (iii) la soluzione proposta; (iv) le misure che siano state già adottate per contenere e limitare le conseguenze della violazione. Il Responsabile del Trattamento garantisce sin d'ora che ogni informazione fornita a tal fine sarà completa, corretta e accurata; inoltre, il Responsabile dovrà adempiere a quanto previsto alla Sezione A4;

- nella redazione della DPIA e nella consultazione preventiva, il Responsabile del trattamento, dovrà assistere il Titolare nella realizzazione delle analisi di impatto relative alla protezione dei dati ai sensi dell'art. 35 del GDPR e nella consultazione preventiva al Garante ai sensi dell'art. 36 del GDPR.

k) ***Cancellazione dei Dati Personali del Titolare.*** Cancellare/distruggere o restituire alla società Titolare (secondo quanto la stessa deciderà e comunicherà al Responsabile del Trattamento di volta in volta) tutti i dati personali dopo la cessazione della prestazione dei Servizi relativi al trattamento e cancellare/distruggere le copie esistenti, documentandone per iscritto l'intervenuta cancellazione/distruzione, salvo che la normativa applicabile preveda la conservazione dei dati.

l) ***Audit.*** Mettere a disposizione del Titolare, dietro semplice richiesta dello stesso, tutta la documentazione e le informazioni necessarie per dimostrare il rispetto degli obblighi stabiliti dall'art. 28 del GDPR e da questo Addendum e consentire e contribuire allo svolgimento delle attività di revisione, comprese le ispezioni, realizzate dal Titolare del Trattamento o da un altro soggetto da questi incaricato. L'audit sarà condotto dal Titolare del Trattamento cercando di limitare al massimo le interferenze con la normale attività di business del Responsabile del Trattamento. Le risultanze dell'audit saranno discusse in buona fede tra le Parti e il Responsabile del Trattamento si impegna sin d'ora ad attuare i cambiamenti ritenuti necessari dal Titolare del Trattamento in seguito all'audit, al fine di garantire la conformità alla Legge Applicabile e all'Addendum.

m) ***DPO***. Comunicare al Titolare del trattamento il nome ed i dati del proprio Responsabile della Protezione dei dati, qualora ne abbia designato uno ai sensi dell'art. 37 del GDPR.

n) ***Registro delle attività di trattamento***. Tenere per iscritto un registro di tutte le categorie di attività di trattamento svolte per conto del Titolare, contenente a) il nome e i dati di contatto del Fornitore quale Responsabile del trattamento, di ogni titolare del trattamento per conto del quale agisce, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati; b) le categorie dei trattamenti effettuati per conto del Titolare e per altri titolari del trattamento; c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, i documenti che attestano l'esistenza di garanzie adeguate; d) ove possibile, una descrizione

generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, del GDPR.

Articolo 5 – Obblighi del Titolare del trattamento

5.1 La società Titolare, quale Titolare del trattamento, è tenuta a:

1) Fornire agli Interessati l'informativa di cui agli articoli 13 e 14 del GDPR;
2) Fornire al Fornitore le informazioni ed i dati elencati nel presente Addendum, nonché ogni altra informazione utile per l'esecuzione delle attività di trattamento illustrate nello stesso;
3) Documentare per iscritto tutte le istruzioni impartite al Responsabile del Trattamento per il trattamento dei Dati Personali del Titolare;
4) Vigilare, in via preventiva e per tutta la durata del trattamento, sul rispetto degli obblighi previsti dal GDPR;
5) Svolgere un'attività di supervisione sul trattamento dei dati personali, ivi incluse le revisioni e le ispezioni di cui al presente Addendum.

Articolo 6 – Conseguenze della violazione delle disposizioni della Legge Applicabile da parte del Responsabile del Trattamento

6.1 Nel caso in cui dovesse violare le disposizioni della Legge Applicabile, determinando le finalità e i mezzi del trattamento, il Fornitore sarà considerato un autonomo titolare del trattamento in questione, fatte salve le disposizioni del GDPR di cui all'art. 82 in tema di diritto al risarcimento e responsabilità, all'art. 83 in tema di condizioni generali per infliggere sanzioni amministrative pecuniarie e all'art. 84 in tema di sanzioni.

Articolo 7 – Clausola di manleva

7.1 Il Fornitore si impegna a manlevare e tenere indenne la società Titolare da qualsiasi danno, pregiudizio, costo, spesa, onere che la stessa dovesse subire e/o dover risarcire a terzi a causa della violazione, da parte del Responsabile del Trattamento, o degli eventuali Sub-Responsabili da esso nominati, delle disposizioni della Legge Applicabile e delle istruzioni impartite dal Titolare del Trattamento.

Articolo 8 – Clausola risolutiva espressa

8.1 Nel caso in cui il Fornitore si rendesse inadempiente ad uno degli obblighi stabiliti all'articolo 4 che precede, il presente Addendum si intenderà risolto ai sensi e per gli effetti di cui all'art. 1456 c.c. dopo che la società Titolare avrà comunicato per iscritto al Fornitore che intende avvalersi della clausola risolutiva espressa, fatto salvo il diritto del Titolare del Trattamento alla manleva ed al risarcimento dei danni conseguenti all'inadempimento.

Articolo 9 – Durata

9.1 Il presente Addendum avrà la stessa durata del Contratto. Lo stesso si intenderà pertanto cessato e/o risolto laddove il Contratto venga a cessare o sia risolto per qualsiasi ragione o causa.

Articolo 10 - Miscellanea

10.1. Per quanto concerne i trattamenti che il Responsabile esegue per conto del Titolare in esecuzione del Contratto, Il Titolare ha facoltà di modificare unilateralmente e discrezionalmente il presente addendum e le istruzioni ivi contenute, mediante apposita comunicazione scritta.
10.2. Le Parti si impegnano a prestare la loro massima cooperazione per modificare o integrare l'Addendum nel caso ciò si renda necessario in virtù di intervenute modifiche nella Legge Applicabile.
10.3. Il presente Addendum e la sua interpretazione ed esecuzione sono regolate dalla Legge Italiana.
10.4. Qualsiasi controversia che dovesse sorgere in connessione o in relazione all'Addendum sarà devoluta alla cognizione esclusiva del Foro previsto nel Contratto.

Per il Titolare del Trattamento	**Per il Responsabile del Trattamento**
Guido Maria Garrone	*Alberto Villa*
Firma:_____	*Firma*:

Ai sensi e per gli effetti di cui all'art. 1341 c.c., il Fornitore dichiara di avere letto e di approvare espressamente le seguenti clausole: art. 7 (Clausola di Manleva); art. 8 (Clausola Risolutiva Espressa); art. 10 (Miscellanea, Foro esclusivo).

Il Fornitore

HQ ENGINEERING ITALIA S.r.l.
Sede Legale e Operativa:
Via Giorgio Stephenson, 29 - 20157 Milano
Tel. 0229062210 - Fax 0262690377
P. IVA 06997160962

SEZIONE A1

ISTRUZIONI PER GLI AMMINISTRATORI DI SISTEMA

Al fine della corretta gestione dei Dati Personali, si invitano gli Amministratori di Sistema (AdS) ad attenersi alle seguenti indicazioni, nonché alle successive eventuali istruzioni.

L'Amministratore di Sistema è tenuto al rispetto delle Policy di sicurezza e protezione dati personali.

All'Amministratore di Sistema è inoltre richiesto di:

- predisporre misure che consentano di sopperire all'eventuale perdita di dati e informazioni o comunque mitigare il rischio di danneggiamento totale o parziale, deterioramento e distruzione delle stesse;
- garantire che i sistemi siano protetti dall'installazione di malware e software non previsti;
- regolare gli accessi a tutte le informazioni per selezione (o per esclusione), secondo la Policy di accessi logici/fisici, nel rispetto dalla Policy di classificazione e a seconda dei ruoli definiti in Azienda;
- rendere i documenti inaccessibili a soggetti privi dell'autorizzazione necessaria per accedervi;
- adottare, nella progettazione di sistemi o infrastrutture ICT, una logica di "privacy by design" basata sul rischio, come da Policy apposita;
- assicurare una gestione di incidenti di sicurezza, ivi comprese violazioni di dati personali, adeguata a consentirne la mitigazione, la segnalazione/comunicazione nei casi previsti dalla legge e prevenirne il ripetersi in futuro, secondo le Policy di gestione incidenti di sicurezza e violazione di dati personali;
- rispettare le Policy di smaltimento o riutilizzo delle apparecchiature informatiche/telematiche e di gestione dei documenti cartacei;
- garantire un'adeguata collaborazione con i responsabili dell'area privacy e/o con le competenti Funzioni aziendali, fornendo supporto, qualora richiesto per i riscontri necessari riguardanti i dati trattati nell'ambito dalla propria designazione quale incaricato, nei modi e nei termini indicati dal proprio Responsabile in Azienda e nel pieno rispetto della legge, in relazione:
- all'esercizio dei diritti dell'Interessato al trattamento dei dati personali, ai sensi del art. 12 del GDPR;
- alle verifiche, controlli e ispezioni previsti dalla Legge, dall'Autorità Garante o dalla Pubblica Amministrazione ed Autorità Giudiziarie e di Polizia;
- seguire scrupolosamente le eventuali ed ulteriori istruzioni fornite dal proprio Responsabile in Azienda e partecipare ai corsi di formazione organizzati dall'Azienda stessa in merito al trattamento dei dati personali.

All'Amministratore di Sistema è infine severamente vietato:

- alterare il funzionamento di componenti software o hardware di un sistema informatico/telematico;
- intervenire senza diritto su dati, informazioni o programmi contenuti in un sistema informatico/telematico al fine di ricavarne un profitto per sé o per terzi;
- compiere attività che possano rendere del tutto o in parte inservibile un sistema informatico/telematico, creare guasti in grado di far scemare le prestazioni del Sistema o comunque qualsiasi azione di annullamento totale di un Sistema;
- diffondere soluzioni software senza prima aver provveduto alla verifica delle stesse mediante software antivirus, antispyware, ecc. opportunamente aggiornati;
- accedere ad aree protette da una qualsivoglia misura di sicurezza (sia essa una misura di protezione logica – ad esempio nome utente e password - o fisica – vigilantes o porte blindate a protezione di sistemi informatici) ove non si abbiano i diritti per accedervi o permanervi oltre la durata stabilita dall'owner del Sistema;
- detenere sulle proprie PDL o diffondere a terze parti non autorizzate codici di accesso (con codici di accesso si intendono non solo password ma anche P.I.N., token software, etc.); ad esempio, è vietato l'export sulla propria postazione, anche se temporaneo, di database contenenti credenziali di accesso ai sistemi;
- diffondere istruzioni tecniche su come eludere od ottenere i suddetti codici di accesso senza autorizzazione del CTO o figura equivalente;
- rivelare il contenuto di documenti riservati;
- utilizzare qualsiasi tecnica finalizzata a carpire dati e informazioni che attraversano una rete telematica (es. Sniffing) senza autorizzazione o per attività non legate alla propria mansione, in special modo nel momento in cui tale attività può comportare un accesso a comunicazioni private tra utenti. Tali tecniche includono l'installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi.

SEZIONE A2

AMBITO del TRATTAMENTO (rif. Art. 3 dell'Addendum)

La presente Sezione costituisce parte integrante dell'Addendum.

Categorie di interessati

- Dipendenti, fornitori di EOLO

Tipo di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati)

- Dati comuni

Natura e finalità del trattamento

- Stipulazione del Contratto ed esecuzione del rapporto contrattuale

Durata del trattamento

- I dati personali saranno trattati per l'intera durata del Contratto e/o dei Servizi e alla cessazione per qualsivoglia motivazione dovranno essere cancellati.

SEZIONE A3

IMPATTI E RISCHI DEL TRATTAMENTO

In linea con il *risk-based approach* di cui al GDPR, Il Titolare ha individuato per le seguenti operazioni di trattamento la necessità di effettuazione di una valutazione d'impatto ed il relativo impatto sui diritti e le libertà degli interessati:

Trattamento	**Impatto**	**Rischio**
Servizi di acquisizione e progettazione siti per la realizzazione di impianti di telecomunicazione	Limitato	Medio

Di seguito si riportano i livelli di impatto e la relativa descrizione:

- Impatto trascurabile: gli interessati dei dati personali coinvolti dal nuovo trattamento non saranno affetti da inconvenienti oppure possono incontrare alcuni inconvenienti che possono superare senza alcun problema (es. ricezione di spam, perdita di tempo per ripetere formalità, etc.);
- Impatto limitato: gli interessati dei dati personali coinvolti dal nuovo trattamento possono incontrare disagi significativi che però possono superare nonostante alcune difficoltà (es. multe imposte erroneamente, account servizi online bloccati, dati non aggiornati, etc.);
- Impatto significativo: gli interessati dei dati personali coinvolti dal nuovo trattamento possono avere conseguenze significative che dovrebbero essere in grado di superare seppure con gravi difficoltà (es. perdita di lavoro, separazione o divorzio, perdita finanziaria a seguito di frode, etc.);
- Impatto massimo: gli interessati dei dati personali coinvolti dal nuovo trattamento possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (es. Perdita di prova nel contesto di contenzioso; Perdita di accesso a infrastrutture vitali, etc.).

Il Responsabile dovrà recepire le modifiche alla presente Sezione A3 a seguito del riesame periodico delle attività di trattamento in capo al Titolare o qualora insorgano variazioni del rischio.

SEZIONE A4

MISURE DI SICUREZZA

La presente Sezione costituisce parte integrante dell'Addendum.

Standard Internazionali

Il Responsabile del trattamento dichiara di fornire, in tema di gestione della sicurezza delle informazioni, servizi conformi ai seguenti standard internazionali:

- ISO 9001:2015 – Sistemi di gestione della qualità – requisiti;
- ISO/IEC 27001:2013 - information security management system;

Misure di sicurezza

Il Responsabile dichiara, per i trattamenti oggetto del Contratto:

- di provvedere alla rimozione dei dati entro i termini definiti nel Contratto fornendo opportuna evidenza dell'avvenuta rimozione. La rimozione dei dati dovrà essere tale da impedire il recupero degli stessi anche tramite attività di *computer forensic*;
- di applicare ai suoi fornitori le medesime misure di sicurezza a esso richieste;
- di implementare tutte le misure di sicurezza previste dalle seguenti normative/provvedimenti:
  - "Rifiuti di apparecchiature elettriche ed elettroniche (RAEE) e misure di sicurezza dei dati personali" - 13 ottobre 2008;
  - Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*", così come modificato dal Provvedimento del Garante del 25 giugno 2009.
- di aver implementato le misure tecnico-organizzative adeguate a soddisfare gli obiettivi di controllo della Sezione A5.

Gestione delle violazioni di dati personali ("*Personal Data Breach*")

Qualunque potenziale violazione di dati personali relativa a riservatezza, integrità, disponibilità e qualità dei dati dovrà essere tempestivamente comunicata al Titolare del trattamento.

Il Responsabile dovrà garantire il supporto al Titolare nelle attività di indagine e *remediation*.

Incident Report

Il Responsabile si impegna a registrare tutte le potenziali violazioni di dati personali, in particolare:

- le modalità di gestione e registrazione delle potenziali violazione di dati personali che interessano l'infrastruttura e le successive azioni di attenuazione;

- le modalità di comunicazione di tutte le informazioni ed evidenze nel caso potenziali violazioni di dati personali interessino anche solo parzialmente le infrastrutture assegnate al Titolare;
- le modalità di comunicazioni di eventuali *remediation plan* che possano interessare anche parzialmente le infrastrutture assegnate al Titolare;
- la comunicazione degli esiti delle revisioni delle analisi dei rischi che incombono sulle infrastrutture di interesse del Titolare a seguito del verificarsi di una potenziali violazione di dati personali.

Incident Notification

Il Responsabile deve garantire:

a) La classificazione della potenziale violazione di dati personali coerente con la classificazione concordata con il Titolare, di seguito riportata:

Classificazione della potenziale violazione di dati personali	**Descrizione**	**Identificabilità interessati**
Alto (critico):	evento estraneo al normale corso dell'attività operativa che coinvolge direttamente o indirettamente la Società e le causa un danno di grave entità o problemi di natura legale.	Dati personali, in chiaro, completi e riconducibili direttamente ai contraenti (es. anagrafica Cliente, dati sensibili, riferimenti bancari, account accesso sistemi).
Medio	evento estraneo al normale corso dell'attività operativa che coinvolge direttamente o indirettamente l'azienda e che si ritiene in grado di provocare il danneggiamento e l'alterazione parziale di dati e informazioni utilizzati nell'ambito dei vari processi aziendali oppure	Dati personali non completi, in chiaro, riconducibili direttamente ai contraenti (es. profilo cliente) *Oppure*

	interrompere l'erogazione di uno o più servizi critici;	Dati personali in chiaro riconducibili indirettamente ai contraenti sulla base di codifiche/informazioni potenzialmente note anche a livello pubblico (es. Codice fiscale, Partita IVA, numerazione telefonica di rete fissa, e-mail, IP ecc.)
Basso	evento, accaduto o minaccioso, estraneo al normale corso delle attività che ha ripercussioni sulla normale attività lavorativa dei singoli dipendenti/collaboratori/utenti/clienti. Tale evento non ha grave influenza sull'attività aziendale complessivamente intesa ma condiziona negativamente i ritmi della normale attività lavorativa.	Dati personali completi (es. anagrafica Cliente, dati sensibili, riferimenti bancari, account accesso sistemi) e non completi (es. numero di telefono, profilo cliente ecc.), riconducibili direttamente ai contraenti ma in forma cifrata.

b) il rispetto delle procedure di *escalation* previste per le varie tipologie di violazione di dati personali riscontrata, come di seguito riportato:

- una prima sommaria comunicazione della potenziale violazione di dati personali dev'essere inviata entro 18 ore dal momento in cui è stato rilevato l'evento da parte del Responsabile, indicando le informazioni previste alla lettera j), articolo 4 dell'Addendum;
- un'ulteriore comunicazione dettagliata della potenziale violazione di dati personali dev'essere inviata entro 48 ore dalla rilevazione dell'evento da parte del Responsabile.

A tal fine si riportano di seguito:

- le modalità attraverso le quali il Titolare può comunicare al Responsabile una potenziale violazione di dati personali rilevata sull'infrastruttura o sui servizi da esso erogati:

- via PEC o e-mail: <hqitalia@legalmail.it> ;

- le modalità attraverso le quali il Responsabile può comunicare al Titolare una potenziale violazione di dati personali rilevata sull'infrastruttura o sui servizi sono indicate nell'Addendum.

c) il supporto in caso vi sia necessità di notifica della violazione di dati personali alle autorità competenti.

Accesso ai locali ed ai sistemi

Il Responsabile deve garantire al Titolare o alle figure da esso ingaggiate, per la verifica e/o l'accertamento di eventuali incidenti di sicurezza o violazione di dati personali, l'accesso ai locali e ai sistemi, nonché l'adeguato supporto durante tutta la fase di analisi dell'incidente.

SEZIONE A5

Nella tabella di seguito riportata vengono descritti gli obiettivi di controllo suddivisi per livello di rischio/impatto secondo lo schema seguente:

Colore	Livello di Rischio	Livello di Impatto
Verde	Basso	Trascurabile
Giallo	Medio	Limitato
Rosso	Alto/Critico	Significativo/Massimo

Security policy and procedures for the protection of personal data

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Security policy and procedures for the protection of personal data	**A.1**	The organization should document its policy with regards to personal data processing as part of its information security policy.	**A.5 Security policy**
L	Security policy and procedures for the protection of personal data	**A.2**	The security policy should be reviewed and revised, if necessary, on an annual basis.	**A.5 Security policy**
M	Security policy and procedures for the protection of personal data	**A.3**	The organization should document a separate dedicated security policy with regard to the processing of personal data. The policy should be approved by management and communicated to all employees and relevant external parties	**A.5 Security policy**
M	Security policy and procedures for the protection of personal data	**A.4**	The security policy should at least refer to: the roles and responsibilities of personnel, the baseline technical and organisation measures adopted for the security of personal data, the data processors or other third parties involved in the processing of personal data.	**A.5 Security policy**
M	Security policy and procedures for the protection of personal data	**A.5**	An inventory of specific policies/procedures related to the security of personal data should be created and maintained, based on the general security policy.	**A.5 Security policy**
H	Security policy and procedures for the protection of personal data	**A.6**	The security policy should be reviewed and revised, if necessary, on a semestral basis.	**A.5 Security policy**

Roles and responsibilities

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Roles and responsibilities	**B.1**	Roles and responsibilities related to the processing of personal data should be clearly defined and allocated in accordance with the security policy.	**A.6.1.1 Information security roles and responsibilities**
L	Roles and responsibilities	**B.2**	During internal re-organizations or terminations and change of employment, revocation of rights and responsibilities with respective hand over procedures should be clearly defined.	**A.6.1.1 Information security roles and responsibilities**
M	Roles and responsibilities	**B.3**	Clear appointment of persons in charge of specific security tasks should be performed, including the appointment of a security officer.	**A.6.1.1 Information security roles and responsibilities**
H	Roles and responsibilities	**B.4**	The security officer should be formally appointed (documented). The tasks and responsibilities of the security officer should also be clearly set and documented.	**A.6.1.1 Information security roles and responsibilities**
H	Roles and responsibilities	**B.5**	Conflicting duties and areas of responsibility, for examples the roles of security officer, security auditor, and DPO, should considered to be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of personal data.	**A.6.1.1 Information security roles and responsibilities**

Access control policy

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Access control policy	**C.1**	Specific access control rights should be allocated to each role (involved in the processing of personal data) following the need to know principle.	**A.9.1.1 Access control policy**
M	Access control policy	**C.2**	An access control policy should be detailed and documented. The organization should determine in this document the appropriate access control rules, access rights and restrictions for specific user roles towards the processes and procedures related to personal data.	**A.9.1.1 Access control policy**
M	Access control policy	**C.3**	Segregation of access control roles (e.g. access request, access authorization, access administration) should be clearly defined and documented.	**A.9.1.1 Access control policy**
H	Access control policy	**C.4**	Roles with excessive access rights should be clearly defined and assigned to limited specific members of staff.	**A.9.1.1 Access control policy**

Resource/asset management

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
Access control policy	Resource/asset management	**D.1**	The organization should have a register of the IT resources used for the processing of personal data (hardware, software, and network). The register could include at least the following information: IT resource, type (e.g. server, workstation), location (physical or electronic). A specific person should be assigned the task of maintaining and updating the register (e.g. IT officer).	**A.8 Asset management**
L	Resource/asset management	**D.2**	IT resources should be reviewed and updated on regular basis (specify) .	**A.8 Asset management**
M	Resource/asset management	**D.3**	Roles having access to certain resources should be defined and documented.	**A.8 Asset management**
H	Resource/asset management	**D.4**	IT resources should be reviewed and updated on an annual basis.	**A.8 Asset management**

Change management

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Change management	**E.1**	The organization should make sure that all changes to the IT system are registered and monitored by a specific person (e.g. IT or security officer). Regular monitoring of this process should take place.	**A. 12.1 Operational procedures and responsibilities**
L	Change management	**E.2**	Software development should be performed in a special environment that is not connected to the IT system used for the processing of personal data. When testing is needed, dummy data should be used (not real data). In cases that this is not possible, specific procedures should be in place for the protection of personal data used in testing.	**A. 12.1 Operational procedures and responsibilities**
M	Change management	**E.3**	A detailed and documented change policy should be in place. It should include: a process for introducing changes, the roles/users that have change rights, timelines for introducing changes. The change policy should be regularly updated.	**A. 12.1 Operational procedures and responsibilities**

Data processors

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Data processors	**F.1**	Formal guidelines and procedures covering the processing of personal data by data processors (contractors/outsourcing) should be defined, documented and agreed between the data controller and the data processor prior to the commencement of the processing activities. These guidelines and procedures should mandatorily establish the same level of personal data security as mandated in the organization's security policy.	**A.15 Supplier relationships**
L	Data processors	**F.2**	Upon finding out of a personal data breach, the data processor shall notify the controller without undue delay.	**A.15 Supplier relationships**
L	Data processors	**F.3**	Formal requirements and obligations should be formally agreed between the data controller and the data processor. The data processor should provide sufficient documented evidence of compliance.	**A.15 Supplier relationships**
M	Data processors	**F.4**	The data controller's organization should regularly audit the compliance of the data processor to the agreed level of requirements and obligations.	**A.15 Supplier relationships**
H	Data processors	**F.5**	The employees of the data processor who are processing personal data should be subject to specific documented confidentiality/ non-disclosure agreements.	**A.15 Supplier relationships**

Incidents handling / Personal data breaches

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Incidents handling / Personal data breaches	**G.1**	An incident response plan with detailed procedures should be defined to ensure effective and orderly response to incidents pertaining personal data.	**A.16 Information security incident management**
L	Incidents handling / Personal data breaches	**G.2**	Personal data breaches should be reported immediately to the management. Notification procedures for the reporting of the breaches to competent authorities and data subjects should be in place, following art. 33 and 34 GDPR.	**A.16 Information security incident management**
M	Incidents handling / Personal data breaches	**G.3**	The incidents' response plan should be documented, including a list of possible mitigation actions and clear assignment of roles.	**A.16 Information security incident management**
H	Incidents handling / Personal data breaches	**G.4**	Incidents and personal data breaches should be recorded along with details regarding the event and subsequent mitigation actions performed.	**A.16 Information security incident management**

Business continuity

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Business continuity	**H.1**	The organization should establish the main procedures and controls to be followed in order to ensure the required level of continuity and availability of the IT system processing personal data (in the event of an incident/personal data breach).	**A. 17 Information security aspects of business continuity management**
M	Business continuity	**H.2**	A BCP should be detailed and documented (following the general security policy). It should include clear actions and assignment of roles.	**A. 17 Information security aspects of business continuity management**
M	Business continuity	**H.3**	A level of guaranteed service quality should be defined in the BCP for the core business processes that provide for personal data security.	**A. 17 Information security aspects of business continuity management**
H	Business continuity	**H.4**	Specific personnel with the necessary responsibility, authority and competence to manage business continuity in the event of an incident/personal data breach should be nominated.	**A. 17 Information security aspects of business continuity management**
H	Business continuity	**H.5**	An alternative facility should be considered, depending on the organization and the acceptable downtime of the IT system.	**A. 17 Information security aspects of business continuity management**

Confidentiality of personnel

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Confidentiality of personnel	**I.1**	The organization should ensure that all employees understand their responsibilities and obligations related to the processing of personal data. Roles and responsibilities should be clearly communicated during the pre-employment and/or induction process.	**A.7 Human resource security**
M	Confidentiality of personnel	**I.2**	Prior to up taking their duties employees should be asked to review and agree on the security policy of the organization and sign respective confidentiality and non-disclosure agreements.	**A.7 Human resource security**
H	Confidentiality of personnel	**I.3**	Employees involved in high risk processing of personal data should be bound to specific confidentiality clauses (under their employment contract or other legal act).	**A.7 Human resource security**

Training

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Training	**J.1**	The organization should ensure that all employees are adequately informed about the security controls of the IT system that relate to their everyday work. Employees involved in the processing of personal data should also be properly informed about relevant data protection requirements and legal obligations through regular awareness campaigns.	**A.7.2.2 Information security awareness, education and training**
M	Training	**J.2**	The organization should have structured and regular training programmes for staff, including specific programmers for the induction (to data protection matters) of newcomers.	**A.7.2.2 Information security awareness, education and training**
H	Training	**J.3**	A training plan with defined goals and objectives should be prepared and executed on an annual basis.	**A.7.2.2 Information security awareness, education and training**

Access control and authentication

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Access control and authentication	K.1	An access control system applicable to all users accessing the IT system should be implemented. The system should allow creating, approving, reviewing and deleting user accounts.	A.9 Access control
L	Access control and authentication	K.2	The use of common user accounts should be avoided. In cases where this is necessary, it should be ensured that all users of the common account have the same roles and responsibilities.	A.9 Access control
L	Access control and authentication	K.3	An authentication mechanism should be in place, allowing access to the IT system (based on the access control policy and system). As a minimum a username/password combination should be used. Passwords should respect a certain (configurable) level of complexity.	A.9 Access control
L	Access control and authentication	K.4	The access control system should have the ability to detect and not allow the usage of passwords that don't respect a certain (configurable) level of complexity.	A.9 Access control
M	Access control and authentication	K.5	A specific password policy should be defined and documented. The policy should include at least password length, complexity, validity period, as well as number of acceptable unsuccessful login attempts.	A.9 Access control
M	Access control and authentication	K.6	User passwords must be stored in a "hashed" form.	A.9 Access control
H	Access control and authentication	K.7	Two-factor authentication should preferably be used for accessing systems that process personal data. The authentication factors could be passwords, security tokens, USB sticks with a secret token, biometrics etc.	A.9 Access control
H	Access control and authentication	K.8	Device authentication should be used to guarantee that the processing of personal data is performed only through specific resources in the network.	A.9 Access control

Logging and monitoring

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Logging and monitoring	**L.1**	Log files should be activated for each system/application used for the processing of personal data. They should include all types of access to data (view, modification, deletion).	**A.12.4 Logging and monitoring**
L	Logging and monitoring	**L.2**	Log files should be timestamped and adequately protected against tampering and unauthorized access. Clocks should be synchronised to a single reference time source	**A.12.4 Logging and monitoring**
M	Logging and monitoring	**L.3**	Actions of the system administrators and system operators, including addition/deletion/change of user rights should be logged.	**A.12.4 Logging and monitoring**
M	Logging and monitoring	**L.4**	There should be no possibility of deletion or modification of log files content. Access to the log files should also be logged in addition to monitoring for detecting unusual activity.	**A.12.4 Logging and monitoring**
M	Logging and monitoring	**L.5**	A monitoring system should process the log files and produce reports on the status of the system and notify for potential alerts.	**A.12.4 Logging and monitoring**

Server/Database security

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Server/Database security	**M.1**	Database and applications servers should be configured to run using a separate account, with minimum OS privileges to function correctly.	**A. 12 Operations security**
L	Server/Database security	**M.2**	Database and applications servers should only process the personal data that are actually needed to process in order to achieve its processing purposes.	**A. 12 Operations security**
M	Server/Database security	**M.3**	Encryption solutions should be considered on specific files or records through software or hardware implementation.	**A. 12 Operations security**
M	Server/Database security	**M.4**	Encrypting storage drives should be considered	**A. 12 Operations security**
M	Server/Database security	**M.5**	Pseudonymization techniques should be applied through separation of data from direct identifiers to avoid linking to data subject without additional information	**A. 12 Operations security**
H	Server/Database security	**M.6**	Techniques supporting privacy at the database level, such as authorized queries, privacy preserving data base querying, searchable encryption, etc., should be considered.	**A. 12 Operations security**

Workstation security

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Workstation security	**N.1**	Users should not be able to deactivate or bypass security settings.	**A. 14.1 Security requirements of information systems**
L	Workstation security	**N.2**	Anti-virus applications and detection signatures should be configured on a weekly basis.	**A. 14.1 Security requirements of information systems**
L	Workstation security	**N.3**	Users should not have privileges to install or deactivate unauthorized software applications.	**A. 14.1 Security requirements of information systems**
L	Workstation security	**N.4**	The system should have session timeouts when the user has not been active for a certain time period.	**A. 14.1 Security requirements of information systems**
L	Workstation security	**N.5**	Critical security updates released by the operating system developer should be installed regularly.	**A. 14.1 Security requirements of information systems**
M	Workstation security	**N.6**	Anti-virus applications and detection signatures should be configured on a daily basis.	**A. 14.1 Security requirements of information systems**
H	Workstation security	**N.7**	It should not be allowed to transfer personal data from workstations to external storage devices (e.g. USB, DVD, external hard drives).	**A. 14.1 Security requirements of information systems**
H	Workstation security	**N.8**	Workstations used for the processing of personal data should preferably not be connected to the Internet unless security measures are in place to prevent unauthorised processing, copying and transfer of personal data on store.	**A. 14.1 Security requirements of information systems**
H	Workstation security	**N.9**	Full disk encryption should be enabled on the workstation operating system drives	**A. 14.1 Security requirements of information systems**

Network/Communication security

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Network/Communication security	**O.1**	Whenever access is performed through the Internet, communication should be encrypted through cryptographic protocols (TLS/SSL).	**A.13 Communications Security**
M	Network/Communication security	**O.2**	Wireless access to the IT system should be allowed only for specific users and processes. It should be protected by encryption mechanisms.	**A.13 Communications Security**
M	Network/Communication security	**O.3**	Remote access to the IT system should in general be avoided. In cases where this is absolutely necessary, it should be performed only under the control and monitoring of a specific person from the organization (e.g. IT administrator/security officer) through pre-defined devices.	**A.13 Communications Security**
M	Network/Communication security	**O.4**	Traffic to and from the IT system should be monitored and controlled through Firewalls and Intrusion Detection Systems.	**A.13 Communications Security**
H	Network/Communication security	**O.5**	Connection to the internet should not be allowed to servers and workstations used for the processing of personal data.	**A.13 Communications Security**
H	Network/Communication security	**O.6**	The network of the information system should be segregated from the other networks of the data controller.	**A.13 Communications Security**
H	Network/Communication security	**O.7**	Access to the IT system should be performed only by pre-authorized devices and terminal using techniques such as MAC filtering or Network Access Control (NAC)	**A.13 Communications Security**

Back-ups

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Back-ups	**P.1**	Backup and data restore procedures should be defined, documented and clearly linked to roles and responsibilities.	**A.12.3 Back-Up**
L	Back-ups	**P.2**	Backups should be given an appropriate level of physical and environmental protection consistent with the standards applied on the originating data.	**A.12.3 Back-Up**
L	Back-ups	**P.3**	Execution of backups should be monitored to ensure completeness.	**A.12.3 Back-Up**
L	Back-ups	**P.4**	Full backups should be carried out regularly.	**A.12.3 Back-Up**
M	Back-ups	**P.5**	Backup media should be regularly tested to ensure that they can be relied upon for emergency use.	**A.12.3 Back-Up**
M	Back-ups	**P.6**	Scheduled incremental backups should be carried out at least on a daily basis.	**A.12.3 Back-Up**
M	Back-ups	**P.7**	Copies of the backup should be securely stored in different locations.	**A.12.3 Back-Up**
M	Back-ups	**P.8**	In case a third party service for back up storage is used, the copy must be encrypted before being transmitted from the data controller.	**A.12.3 Back-Up**
H	Back-ups	**P.9**	Copies of backups should be encrypted and securely stored offline as well.	**A.12.3 Back-Up**

Mobile/Portable devices

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Mobile/Portable devices	**Q.1**	Mobile and portable device management procedures should be defined and documented establishing clear rules for their proper use.	**A. 6.2 Mobile devices and teleworking**
L	Mobile/Portable devices	**Q.2**	Mobile devices that are allowed to access the information system should be pre-registered and pre-authorized.	**A. 6.2 Mobile devices and teleworking**
L	Mobile/Portable devices	**Q.3**	Mobile devices should be subject to the same levels of access control procedures (to the data processing system) as other terminal equipment.	**A. 6.2 Mobile devices and teleworking**
M	Mobile/Portable devices	**Q.4**	Specific roles and responsibilities regarding mobile and portable device management should be clearly defined.	**A. 6.2 Mobile devices and teleworking**
M	Mobile/Portable devices	**Q.5**	The organization should be able to remotely erase personal data (related to its processing operation) on a mobile device that has been compromised.	**A. 6.2 Mobile devices and teleworking**
M	Mobile/Portable devices	**Q.6**	Mobile devices should support separation of private and business use of the device through secure software containers.	**A. 6.2 Mobile devices and teleworking**
M	Mobile/Portable devices	**Q.7**	Mobile devices should be physically protected against theft when not in use.	**A. 6.2 Mobile devices and teleworking**
H	Mobile/Portable devices	**Q.8**	Two factor authentication should be considered for accessing mobile devices	**A. 6.2 Mobile devices and teleworking**
H	Mobile/Portable devices	**Q.9**	Personal data stored at the mobile device (as part of the organization's data processing operation) should be encrypted.	**A. 6.2 Mobile devices and teleworking**

Application lifecycle security

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Application lifecycle security	**R.1**	During the development lifecycle best practises, state of the art and well acknowledged secure development practices, frameworks or standards should be followed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
L	Application lifecycle security	**R.2**	Specific security requirements should be defined during the early stages of the development lifecycle.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
L	Application lifecycle security	**R.3**	Specific technologies and techniques designed for supporting privacy and data protection (also referred to as Privacy Enhancing Technologies (PETs)) should be adopted in analogy to the security requirements.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
L	Application lifecycle security	**R.4**	Secure coding standards and practises should be followed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
L	Application lifecycle security	**R.5**	During the development, testing and validation against the implementation of the initial security requirements should be performed.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
M	Application lifecycle security	**R.6**	Vulnerability assessment, application and infrastructure penetration testing should be performed by a trusted third party prior to the operational adoption. The application shall not be adopted unless the required level of security is achieved.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
M	Application lifecycle security	**R.7**	Periodic penetration testing should be carried out.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
M	Application lifecycle security	**R.8**	Information about technical vulnerabilities of information systems being used should be obtained.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**
M	Application lifecycle security	**R.9**	Software patches should be tested and evaluated before they are installed in an operational environment.	**A.12.6 Technical vulnerability management & A.14.2 Security in development and support processes**

Data deletion/disposal

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Data deletion/disposal	**S.1**	Software-based overwriting should be performed on all media prior to their disposal. In cases where this is not possible (CD's, DVD's, etc.) physical destruction should be performed.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or reuse of equipment**
L	Data deletion/disposal	**S.2**	Shredding of paper and portable media used to store personal data shall be carried out.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or reuse of equipment**
M	Data deletion/disposal	**S.3**	Multiple passes of software-based overwriting should be performed on all media before being disposed.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or reuse of equipment**
M	Data deletion/disposal	**S.4**	If a third party's services are used to securely dispose of media or paper based records, a service agreement should be in place and a record of destruction of records should be produced as appropriate.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or reuse of equipment**
H	Data deletion/disposal	**S.5**	Following the software erasure, additional hardware based measures such as degaussing should be performed. Depending on the case, physical destruction should also be considered.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or reuse of equipment**
H	Data deletion/disposal	**S.6**	If a third party, therefor data processor, is being used for destruction of media or paper based files, it should be considered that the process takes place at the premises of the data controller (and avoid off-site transfer of personal data.	**A. 8.3.2 Disposal of media & A. 11.2.7 Secure disposal or reuse of equipment**

Physical security

LEVEL	MEASURE CATEGORY	MEASURE	MEASURE DESCRIPTION	RELEVANT ISO/IEC 27001: 2013 CONTROL
L	Physical security	**T.1**	The physical perimeter of the IT system infrastructure should not be accessible by non-authorized personnel.	**A.11 – Physical and environmental security**
M	Physical security	**T.2**	Clear identification, through appropriate means e.g. ID Badges, for all personnel and visitors accessing the premises of the organization should be established, as appropriate.	**A.11 – Physical and environmental security**
M	Physical security	**T.3**	Secure zones should be defined and be protected by appropriate entry controls. A physical log book or electronic audit trail of all access should be securely maintained and monitored	**A.11 – Physical and environmental security**
M	Physical security	**T.4**	Intruder detection systems should be installed in all security zones.	**A.11 – Physical and environmental security**
M	Physical security	**T.5**	Physical barriers should, where applicable, be built to prevent unauthorized physical access.	**A.11 – Physical and environmental security**
M	Physical security	**T.6**	Vacant secure areas should be physically locked and periodically reviewed	**A.11 – Physical and environmental security**
M	Physical security	**T.7**	An automatic fire suppression system, closed control dedicated air conditioning system and uninterruptible power supply (UPS) should be implemented at the server room	**A.11 – Physical and environmental security**
M	Physical security	**T.8**	External party support service personnel should be granted restricted access to secure areas.	**A.11 – Physical and environmental security**

HQ ENGINEERING ITALIA S.r.l.
Sede Legale e Operativa:
Via Giorgio Stephenson, 29 - 20157 Milano
Tel. 0229062210 - Fax 0262690377
P. IVA 06997160962