ALLEGATO A
ACCORDO IN MERITO AL TRATTAMENTO DI DATI PERSONALI
ai sensi dell'art. 28 del Regolamento (UE) 2016/679

SEZIONE I

1. Scopo e ambito di applicazione

(a) Scopo del presente accordo è garantire il rispetto dell'articolo 28, paragrafi 3 e 4, 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. Il titolare del trattamento[1] (nel proseguio anche Cliente) e il responsabile del trattamento (Project Informatica Srl Unipersonale, nel proseguio anche Project) (nel prosieguo entrambe anche le "Parti"), di cui al Corpo Offerta, hanno accettato le presenti clausole al fine di garantire il rispetto dell'articolo 28, paragrafi 3 e 4, del Regolamento (UE) 2016/679.

(b) Le presenti clausole si applicano al trattamento dei dati personali specificato alla Sezione IV.

(c) Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il titolare del trattamento a norma del Regolamento (UE) 2016/679, del D.lgs. 196/2003 e di altre disposizioni applicabili, nazionali o dell'Unione europea, relative alla protezione dei dati.

(d) Le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al capo V del Regolamento (UE) 2016/679.

2. Invariabilità delle clausole

Le Parti si impegnano a non modificare le clausole se non per aggiungere o aggiornare informazioni nelle Sezioni IV, V e VI. Ciò non impedisce alle Parti di includere le clausole stabilite nel presente documento in un contratto più ampio o di aggiungere altre clausole o garanzie supplementari, purché queste non contraddicano, direttamente o indirettamente, le presenti clausole o ledano i diritti o le libertà fondamentali degli interessati.

3. Interpretazione

(a) Quando le presenti clausole utilizzano i termini definiti nel Regolamento (UE) 2016/679, tali termini hanno lo stesso significato di cui al regolamento predetto.

(b) Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del Regolamento (UE) 2016/679.

(c) Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal Regolamento (UE) 2016/679, o che pregiudichi i diritti o le libertà fondamentali degli interessati.

4. Prevalenza

(a) Come previsto dalle Condizioni Generali, il presente documento si ritiene integralmente accettato se, entro 15 (quindici) giorni dalla sottoscrizione delle stesse, il Cliente non sottopone a Project un diverso *template* di Nomina a Responsabile del Trattamento dei dati personali. Resta ferma la verifica preventiva del *template* ricevuto dal Cliente, prima della relativa sottoscrizione.

(b) Si precisa sin d'ora che, previa sottoscrizione del documento di cui alla lett.(a) da parte di Project, l'Allegato A si ritiene sostituito da quest'ultimo.

SEZIONE II - OBBLIGHI DELLE PARTI

5. Descrizione del trattamento

I dettagli dei trattamenti, in particolare le categorie di dati personali e le finalità del trattamento per le quali i dati personali sono trattati per conto del titolare del trattamento, sono specificati nella Sezione IV.

6. Obblighi delle Parti

6.1. Istruzioni

(a) Il responsabile del trattamento tratta i dati personali soltanto su istruzione documentata del titolare del trattamento, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento. In tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto lo vieti per rilevanti motivi di interesse pubblico. Il titolare del trattamento può anche impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate.

(b) Il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, le istruzioni del titolare del trattamento violino il Regolamento (UE) 2016/679, il D.lgs. 196/2003 o altre disposizioni applicabili, nazionali o dell'Unione europea, relative alla protezione dei dati.

6.2. Limitazione delle finalità

Il responsabile del trattamento tratta i dati personali soltanto per le finalità specifiche del trattamento di cui alla Sezione IV, salvo ulteriori istruzioni del titolare del trattamento.

6.3. Durata del trattamento dei dati personali

Il responsabile del trattamento tratta i dati personali soltanto per la durata specificata nella Sezione IV.

[1] Si intenda la persona giuridica che gode del Servizio.

6.4. Sicurezza del trattamento

(a) Il responsabile del trattamento mette in atto almeno le misure tecniche e organizzative specificate nella Sezione V per garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le Parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

(b) Il responsabile del trattamento concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del Contratto. Il responsabile del trattamento garantisce che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

(c) Come indicato nell'art. 2-quaterdecies, comma 2 del decreto legislativo n. 196/2003, il responsabile del trattamento può individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la sua autorità. Tuttavia, è necessario che il responsabile del trattamento sia in grado di dimostrare di aver istruito adeguatamente le persone autorizzate al trattamento, in particolare in relazione ai principi fondamentali in materia di trattamento dei dati personali di cui all'art. 5 del Regolamento (UE) 2016/679.

6.5. Dati particolari e dati giudiziari

Se il trattamento riguarda dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici o dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati relativi a condanne penali e a reati, il responsabile del trattamento, se messo a conoscenza da parte del titolare del trattamento in merito alla categoria dei dati di cui al presente punto oggetto di trattamento, applica limitazioni specifiche e/o garanzie supplementari.

6.6 Documentazione e rispetto

(a) Le Parti devono essere in grado di dimostrare il rispetto delle presenti clausole.

(b) Il responsabile del trattamento risponde prontamente e adeguatamente alle richieste di informazioni del titolare del trattamento relative al trattamento dei dati conformemente alle presenti clausole.

(c) Il responsabile del trattamento mette a disposizione del titolare del trattamento tutte le informazioni necessarie a dimostrare il rispetto degli obblighi stabiliti nelle presenti clausole e che derivano direttamente dal Regolamento (UE) 2016/679, dal D.lgs. 196/2003 e da altre disposizioni applicabili, nazionali o dell'Unione europea, relative alla protezione dei dati.

(d) Su richiesta del titolare del trattamento, il responsabile del trattamento consente e contribuisce alle attività di revisione delle attività di trattamento di cui alle presenti clausole, a intervalli ragionevoli o se vi sono indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il titolare del trattamento può tenere conto delle pertinenti certificazioni in possesso del responsabile del trattamento.

(e) Il titolare del trattamento può scegliere di condurre l'attività di revisione autonomamente o incaricare un revisore indipendente. Le attività di revisione possono comprendere anche ispezioni nei locali o nelle strutture fisiche del responsabile del trattamento e, se del caso, sono effettuate con un preavviso ragionevole.

(f) Su richiesta, le Parti mettono a disposizione della o delle autorità di controllo competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione.

6.7. Ricorso a sub-responsabili del trattamento

(a) Il responsabile del trattamento ha l'autorizzazione generale del titolare del trattamento per ricorrere a sub-responsabili del trattamento. Su richiesta del titolare del trattamento, Project fornirà l'elenco dei sub-responsabili implicati in specifiche attività di trattamento, nonché eventuali variazioni.

(b) Qualora il responsabile del trattamento ricorra a un sub-responsabile del trattamento per l'esecuzione di specifiche attività di trattamento, il responsabile del trattamento stipula un contratto con il sub-responsabile che imponga a quest'ultimo, nella sostanza, gli stessi obblighi in materia di protezione dei dati imposti al responsabile del trattamento conformemente alle presenti clausole. Il responsabile del trattamento si assicura che il sub-responsabile del trattamento rispetti gli obblighi cui il responsabile del trattamento è soggetto a norma delle presenti clausole e del Regolamento (UE) 2016/679, del D.lgs. 196/2003 e di altre disposizioni applicabili, nazionali o dell'Unione europea, relative alla protezione dei dati.

(c) Il responsabile del trattamento rimane pienamente responsabile nei confronti del titolare del trattamento dell'adempimento degli obblighi del sub-responsabile del trattamento derivanti dal contratto che questi ha stipulato con il responsabile del trattamento. Il responsabile del trattamento notifica al titolare del trattamento qualunque inadempimento, da parte del sub-responsabile del trattamento, degli obblighi contrattuali.

6.8. Trasferimenti internazionali

(a) Qualunque trasferimento di dati verso un paese terzo al di fuori dello Spazio Economico Europeo (SEE) o verso un'organizzazione internazionale da parte del responsabile del trattamento è effettuato soltanto nel rispetto delle disposizioni di cui al capo V del Regolamento (UE) 2016/679, affinché sia garantito un livello di protezione dei dati equivalente a quello previsto dal Regolamento (UE) 2016/679. Su richiesta del titolare del trattamento, il responsabile del trattamento informa il primo relativamente ad eventuali trasferimenti di dati personali trattati nell'ambito del presente accordo al di fuori del SEE o verso un'organizzazione internazionale, e fornisce al titolare prova del rispetto delle disposizioni di cui al capo V

del Regolamento (UE) 2016/679. Qualora il titolare del trattamento ravvisi il mancato rispetto delle disposizioni di cui al capo V del Regolamento (UE) 2016/679, il responsabile del trattamento non può trasferire i dati al di fuori del SEE o verso un'organizzazione internazionale.

7. Assistenza al titolare del trattamento

(a) Il responsabile del trattamento notifica prontamente al titolare del trattamento qualunque richiesta ricevuta dall'interessato. Non risponde egli stesso alla richiesta, a meno che sia stato autorizzato in tal senso dal titolare del trattamento.

(b) Il responsabile del trattamento assiste il titolare del trattamento nell'adempimento degli obblighi di rispondere alle richieste degli interessati per l'esercizio dei loro diritti, tenuto conto della natura del trattamento. Nell'adempiere agli obblighi di cui alle lettere a) e b), il responsabile del trattamento si attiene alle istruzioni del titolare del trattamento.

(c) Oltre all'obbligo di assistere il titolare del trattamento in conformità della clausola 7, lett. b), il responsabile del trattamento assiste il primo anche nel garantire il rispetto degli obblighi di cui agli artt. da 32 a 36 Regolamento (UE) 2016/679.

8. Notifica di una violazione dei dati personali

In caso di violazione dei dati personali, il responsabile del trattamento coopera con il titolare del trattamento e lo assiste nell'adempimento degli obblighi che incombono a quest'ultimo a norma degli articoli 33 e 34 del Regolamento (UE) 2016/679, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.

8.1 Violazione riguardante dati trattati dal titolare del trattamento

In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:

(a) nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza;

(b) nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del Regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:

(1) la natura dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

(2) le probabili conseguenze della violazione dei dati personali;

(3) le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

(c) nell'adempiere, in conformità dell'articolo 34 del Regolamento (UE) 2016/679, all'obbligo di comunicare senza ingiustificato ritardo la violazione dei dati personali all'interessato, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

8.2 Violazione riguardante dati trattati dal responsabile del trattamento

In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento entro quarantotto (48) ore dal momento in cui ne è venuto a conoscenza. La notifica contiene almeno:

(a) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);

(b) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;

(c) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.

Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.

SEZIONE III - DISPOSIZIONI FINALI

9. Inosservanza delle clausole e risoluzione

(a) Fatte salve le disposizioni del Regolamento (UE) 2016/679, qualora il responsabile del trattamento violi gli obblighi che gli incombono a norma delle presenti clausole, il titolare del trattamento può dare istruzione al responsabile del trattamento di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole o non sia risolto il Contratto. Il responsabile del trattamento informa prontamente il titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

(b) Il titolare del trattamento ha diritto di risolvere il Contratto per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole qualora:

(1) il trattamento dei dati personali da parte del responsabile del trattamento sia stato sospeso dal titolare del trattamento in conformità della lettera a) e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione;

(2) il responsabile del trattamento violi in modo sostanziale o persistente le presenti clausole o gli obblighi che gli incombono a norma del Regolamento (UE) 2016/679;

(3) il responsabile del trattamento non rispetti una decisione vincolante di un organo giurisdizionale competente o della o delle autorità di controllo competenti per quanto riguarda i suoi obblighi in conformità delle presenti clausole o del Regolamento (UE) 2016/679 o del D.lgs. 196/2003 e di altre disposizioni applicabili, nazionali o dell'Unione europea, relative alla protezione dei dati.

(c) Il responsabile del trattamento ha diritto di risolvere il Contratto per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole qualora, dopo aver informato il titolare del trattamento che le sue istruzioni violano i requisiti giuridici applicabili in conformità della clausola 6.1, lett. b), il titolare del trattamento insista sul rispetto delle istruzioni.

(d) Dopo la risoluzione del Contratto il responsabile del trattamento, a scelta del titolare del trattamento, cancella tutti i dati personali trattati per conto del titolare del trattamento e certifica a quest'ultimo di averlo fatto, oppure restituisce al titolare del trattamento tutti i dati personali e cancella le copie esistenti, a meno che il diritto dell'Unione europea o dello Stato membro non richieda la conservazione dei dati personali. Finché i dati non sono cancellati o restituiti, il responsabile del trattamento continua ad assicurare il rispetto delle presenti clausole.

SEZIONE IV: DESCRIZIONE DEL TRATTAMENTO EFFETTUATO DAL RESPONSABILE DEL TRATTAMENTO

10. Finalità del trattamento

Il Cliente è consapevole che la finalità del trattamento dei dati raccolti corrisponde unicamente alla necessità derivante dalle prestazioni oggetto dell'offerta di cui alla Sezione I.

11. Categorie di interessati

Le categorie di interessati i cui dati personali sono trattati da Project, per qualsivoglia Servizio, sono le seguenti:

(a) Utenti

(b) Personale in forza[2]

12. Categorie di dati personali e Natura del trattamento

12.1 Le categorie di dati personali trattati da Project sono quelle indicate nella tabella sottoriportata; nel caso in cui siano trattate ulteriori e/o differenti categorie di dati personali, sarà onere del titolare del trattamento comunicare eventuali variazioni come da punto 14 del presente documento.

12.2 La tabella sottoriportata descrive inoltre le tipologie di natura del trattamento relativamente ad ogni servizio per il quale Project risulti responsabile del trattamento. Pertanto, si precisa che il Cliente dovrà ritenere applicabile solo quanto riferito ai Servizi presenti in corpo offerta.

[2] Per "Utenti" e "Personale in forza" si intende: Dipendenti, Collaboratori, Clienti e Fornitori.

Servizio	Categorie di dati personali trattati dal responsabile del trattamento	Natura del trattamento
ADVANCED RECOVERY	Dati Utente[3] Credenziali[4]	conservazione consultazione
DISASTER RECOVERY		
AWS PPU SERVICES (terzi)		
GOOGLE CLOUD PLATFORM (GCP) (terzi)		
IAAS (terzi)		
MANAGED SUPPORT INFRASTRUCTURE		
MANAGED SUPPORT INFRASTRUCTURE (terzi)		
MANAGED SUPPORT SISTEMI OPERATIVI E SERVIZI CORE		
MANAGED SUPPORT SISTEMI OPERATIVI E SERVIZI CORE (terzi)		
MSP STRONG AUTHENTICATION		
PATCH MANAGEMENT PLAN (ADD-ON)		
RMM SERVER		
RMM SERVER WITH MONITORAGGIO		
RMM WORKPLACE		
WASABI CLOUD STORAGE (Terzi)		
CSP OFFICE 365 PROFILO BASE		
CSP OFFICE 365 PROFILO MANAGED		
MS AZURE PROFILO BASE		
MS AZURE PROFILO MANAGED		
NOC LICENSING & SUPPORT		
NOC MONITORING		
NOC MONITORING H24		
NOC MONITORING H24 SOLO PRESIDIO		
IAAS		
SOC (Terzi)	Log[5]	raccolta conservazione estrazione consultazione comunicazione
SOC		
XDR MANAGEMENT	Credenziali Log	
DARK WEB MONITORING	Dati Utente	raccolta organizzazione comunicazione conservazione consultazione
MSP ANTISPAM	Dati Utente Credenziali Log	consultazione conservazione raccolta
NOC BACKUP MANAGEMENT	Credenziali	conservazione consultazione
NOC BACKUP MANAGEMENT PLUS		
MANAGED SUPPORT NETWORK		
MANAGED SUPPORT NETWORK (terzi)		
MANAGEMENT FIREWALL SERVICE		
MANAGEMENT SECURITY APPLIANCE		
WEB FILTERING	Credenziali Log	raccolta conservazione consultazione

[3] Per "Dati Utente" si intende potenzialmente tutti le informazioni digitali memorizzate o in transito sui sistemi del Cliente oggetto del Servizio, come, a titolo esemplificativo e non esaustivo, dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale), dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile).

[4] Per "Credenziale" si intende username, password ed eventuali sistemi di MFA creati ad hoc per l'amministrazione dei sistemi del Cliente. Si precisa che l'utenza in questione è ad uso esclusivo di Project al fine di erogare il Servizio. Non sono pertanto oggetto di trattamento credenziali personali ovvero amministrativi in uso diretto del Cliente.

[5] Per "Log" si intende tutte le informazioni che tracciano accessi e/o attività informatiche sui sistemi del Cliente oggetto del Servizio.

LOG MANAGEMENT	Log	raccolta conservazione estrazione consultazione comunicazione
Active Directory Security Assessment	Dati Utente Log Credenziali	raccolta registrazione organizzazione conservazione estrazione consultazione comunicazione
CIS Critical Security Controls Framework Nazionale per la Cybersecurity e la Data Protection (FNCDP v.2.1 2025)	Dati Utente	raccolta registrazione organizzazione conservazione consultazione comunicazione raffronto
External Network Penetration Test Internal Attacker Simulation External Network Vulnerability Assessment Internal Network Vulnerability Assessment Wireless Network Vulnerability Assessment General Phishing Spear Phishing	Dati Utente Log Credenziali	raccolta registrazione organizzazione conservazione estrazione consultazione comunicazione raffronto
O365 Security Assessment	Dati Utente Credenziali	conservazione estrazione consultazione comunicazione
Security Events Analysis	Log	raccolta conservazione estrazione consultazione comunicazione
Osint	Dati Utente	raccolta organizzazione comunicazione conservazione consultazione
Web Application Security Assessment	Dati Utente Log Credenziali (esclusivamente per le formule “grey box” e “white box”)	raccolta registrazione organizzazione conservazione estrazione consultazione comunicazione raffronto
SOFTWARE WEB SOFTWARE WEB (Terzi)	Dati Utente Log Credenziali	raccolta registrazione organizzazione strutturazione conservazione adattamento o modifica (Log esclusi) estrazione consultazione comunicazione raffronto interconnessione limitazione cancellazione distruzione

INCIDENT RESPONSE	Log Dati Utente Credenziali	raccolta registrazione organizzazione conservazione estrazione consultazione comunicazione
PLAFOND SERVIZI IT PACCHETTO ORE AI ADVISORY AI MANTENAINCE & SUPPORT AI POC AI PROJECT	Il trattamento dei dati sarà potenzialmente relativo a differenti categorie, conservati nei sistemi informatici del titolare del trattamento Quest'ultimo provvederà pertanto a dare dovute istruzioni a Project una volta individuate le suddette categorie. Il trattamento dei dati sarà potenzialmente relativo a differenti categorie, conservati nei sistemi informatici del titolare del trattamento Quest'ultimo provvederà pertanto a dare dovute istruzioni a Project una volta individuate le suddette categorie.	In ragione della natura del Contratto non è possibile individuare preventivamente la natura del trattamento. Il titolare del trattamento provvederà pertanto a dare dovute istruzioni a Project una volta individuate quali tra le seguenti sono le attività di trattamento applicabili: - Raccolta - Registrazione - Organizzazione - Strutturazione - Conservazione - Adattamento o modifica - Estrazione - Consultazione - Comunicazione - Diffusione - Raffronto - Interconnessione - Limitazione - Cancellazione - Distruzione

13. Durata del Trattamento

Il trattamento può essere effettuato dal responsabile del trattamento fino alla conclusione del Servizio. Sono fatti salvi gli obblighi di trattamento dei dati personali imposti da disposizioni di legge che prevedano un periodo di trattamento ulteriore da parte del responsabile del trattamento.

14. Variazioni

Si precisa che, nel caso in cui il Cliente riscontri un'incongruenza rispetto a quanto esposto nella presente Sezione, sarà suo onere comunicare eventuali variazioni e/o integrazioni relativamente a:

(a) Finalità del trattamento;
(b) Categorie di dati personali trattati;
(c) Categorie di interessati coinvolti;
(d) Natura del trattamento;
(e) Durata del trattamento.

Le richieste di cui sopra dovranno esser formalmente precisate dal Cliente medesimo e, previa accettazione, figureranno quale parte integrante del Contratto.

SEZIONE V: MISURE TECNICHE E ORGANIZZATIVE, COMPRESE MISURE TECNICHE E ORGANIZZATIVE PER GARANTIRE LA SICUREZZA DEI DATI

- Esiste ed è mantenuto aggiornato un inventario dei sistemi, dispositivi, software, servizi e applicazioni informatiche in uso all'interno del perimetro aziendale.
- I servizi web (social network, cloud computing, posta elettronica, spazio web, ecc.) offerti da Terzi a cui si è registrati sono quelli strettamente necessari.
- Sono individuate le informazioni, i dati e i sistemi critici per l'azienda affinché siano adeguatamente protetti.
- È stato nominato un referente che sia responsabile per il coordinamento delle attività di gestione e di protezione delle informazioni e dei sistemi informatici.
- Sono identificate e rispettate le leggi e/o i regolamenti con rilevanza in tema di protezione dei dati personali e cybersecurity che risultino applicabili per l'azienda.
- Tutti i dispositivi che lo consentono sono dotati di software di protezione (ad es. antivirus, antimalware) regolarmente aggiornato.
- Le password sono diverse per ogni account, della complessità adeguata e viene valutato l'utilizzo dei sistemi di autenticazione più sicuri offerti dal Provider del servizio (ad es. autenticazione a due fattori).
- Il personale autorizzato all'accesso, remoto o locale, ai servizi informatici dispone di utenze personali non condivise con altri; l'accesso è opportunamente protetto; i vecchi account non più utilizzati sono disattivati.
- Ogni utente può accedere solo alle informazioni e ai sistemi di cui necessita e/o di sua competenza.

- Il personale è adeguatamente sensibilizzato e formato sui rischi di cybersecurity e sulle pratiche da adottare per l'impiego sicuro degli strumenti aziendali.
- I vertici aziendali hanno cura di predisporre per tutto il personale aziendale la formazione necessaria a fornire almeno le nozioni basilari di sicurezza e protezione dei dati personali.
- La configurazione iniziale di tutti i sistemi e dispositivi è svolta da personale esperto, responsabile per la configurazione sicura degli stessi. Le credenziali di accesso di default sono sempre sostituite.
- Sono eseguiti periodicamente backup delle informazioni e dei dati critici per l'azienda. I backup sono conservati in modo sicuro e verificati periodicamente.
- Le reti e i sistemi sono protetti da accessi non autorizzati attraverso strumenti specifici (ad es: Firewall e altri dispositivi/software anti-intrusione).
- In caso di incidente informatico vengono informati i responsabili della sicurezza e i sistemi vengono messi in sicurezza da personale esperto.
- Tutti i software in uso (inclusi i firmware) sono aggiornati all'ultima versione consigliata dal produttore. I dispositivi o i software obsoleti e non più aggiornabili sono dismessi.

In conformità alla clausola 7.4 lett. a) del presente accordo contrattuale, il responsabile del trattamento si impegna inoltre a garantire l'adozione di ulteriori misure di sicurezza - tecniche e organizzative - che siano necessarie a garantire un livello di sicurezza dei dati adeguato ai rischi per i diritti e le libertà degli interessati.

SEZIONE VI: ISTRUZIONI DEL TITOLARE DEL TRATTAMENTO NEI CONFRONTI DEL RESPONSABILE DEL TRATTAMENTO

Il responsabile del trattamento individuato (nel prosieguo, anche il "responsabile") è tenuto ad effettuare i trattamenti dei dati nel rispetto di quanto disposto dalla normativa vigente, di ulteriori ed eventuali contenuti specifici di cui all'accordo contrattuale cui il presente allegato si riferisce, secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità degli interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.
Il responsabile è tenuto a trattare i dati personali nel rispetto dei principi di necessità, proporzionalità e minimizzazione dei dati, in modo lecito e secondo correttezza, per scopi legittimi e determinati, assicurando l'esattezza e la completezza dei dati. Il responsabile è tenuto ad iniziare eventuali nuovi trattamenti dei dati di cui alla Sezione IV solo in seguito a richiesta da parte del titolare del trattamento (nel prosieguo, anche il "titolare").
Il responsabile, in relazione ai soggetti autorizzati al trattamento che agiscono sotto la sua autorità, è tenuto a:

1) individuare per iscritto i soggetti autorizzati (persone fisiche o gruppi omogenei);
2) impartire ai soggetti autorizzati le istruzioni idonee alle attività di trattamento da svolgere;
3) vigilare sull'operato dei soggetti autorizzati;
4) prevedere un piano di formazione destinato ai soggetti autorizzati;
5) assicurarsi che ad ogni soggetto autorizzato sia assegnata una credenziale di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione del soggetto autorizzato al trattamento associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'autorizzato, eventualmente associato a un codice identificativo o a una parola chiave. Ove possibile, il responsabile adotta sistemi di autenticazione a più fattori e, in assenza, richiede la definizione di password forti (ad es. almeno 14 caratteri)
6) assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza;
7) impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo;
8) prescrivere necessarie cautele per assicurare la segretezza della componente riservata della credenziale e/o la diligente custodia del dispositivo in possesso ed uso esclusivo dei soggetti autorizzati al trattamento;
9) assicurare che il codice per l'identificazione, laddove utilizzato, non possa essere assegnato ad altri autorizzati, neppure in tempi diversi;
10) assicurare che sia operata la disattivazione delle credenziali di autenticazione del personale in caso venga a cessare la necessità di accesso da parte del soggetto autorizzato al trattamento o intervenga un'inattività per più di 180 giorni;
11) predisporre le necessarie procedure affinché, in caso di prolungata assenza o impedimento dell'autorizzato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, si possa comunque assicurare la disponibilità di dati o strumenti elettronici. In tal caso la custodia delle copie delle credenziali deve essere organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti deputati alla loro custodia;
12) prevedere, con criteri restrittivi, profili di autorizzazione di accesso per ogni singolo soggetto autorizzato al trattamento o gruppo omogeneo e configurarli prima dell'inizio dei trattamenti;
13) verificare, ad intervalli almeno annuali, le autorizzazioni in essere;
14) assicurare che nel caso di operatori telefonici, autorizzati al trattamento, questi nelle comunicazioni vocali scambiate durante lo svolgimento delle proprie attività si conformino alle disposizioni specificatamente predisposte dal responsabile del trattamento per il rispetto dell'utenza e la riservatezza delle informazioni trattate;
15) redigere e mantenere aggiornato un elenco con gli estremi identificativi delle persone fisiche che rivestono il ruolo di Amministratori di Sistema e, per ciascuno di essi, la descrizione delle funzioni che gli sono state attribuite nell'ambito delle attività svolte per conto del titolare e implementare le ulteriori misure di sicurezza, come definito nel provvedimento del Garante per la protezione dei dati personali del 27/11/2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici

relativamente alle attribuzioni delle funzioni di amministratori di sistema" e s.m.i. (pubblicato in G.U. n. 300 del 24 dicembre 2008 e modificato con provvedimento del 25 giugno 2009);

16) provvedere, ogni qualvolta vi sia la segnalazione della presenza di vulnerabilità nei programmi utilizzati e la contemporanea disponibilità delle opportune modifiche, al tempestivo aggiornamento dei programmi;
17) prevedere l'adozione di copie di back-up e il ripristino dei dati in tempi certi e comunque non superiori a sette giorni.

Il responsabile deve assicurare che gli interessati possano esercitare i diritti di cui al Capo III del Regolamento (UE) 2016/679, nel rispetto dei termini di legge, adottando ogni soluzione organizzativa, logistica, tecnica e procedurale idonea ad assicurare l'osservanza delle disposizioni vigenti in materia di trattamento dei dati personali per l'esercizio degli stessi diritti. Nel caso in cui il responsabile riceva da parte dell'interessato una istanza per l'esercizio dei suoi diritti ai sensi degli artt. da 15 a 22 del Regolamento (UE) 2016/679, è tenuto ad inoltrarla prontamente al titolare in quanto individuato quale soggetto tenuto alla evasione della stessa.

In merito al trattamento dei dati personali con strumenti diversi da quelli elettronici, il responsabile è tenuto a predisporre un archivio per gli atti e i documenti con dati personali individuando per iscritto i soggetti autorizzati al trattamento con i relativi profili di accesso ai dati ed ai documenti. Devono essere definite le procedure di deposito, custodia, consegna o restituzione e compartimentazione dei dati stessi (ad esempio, un registro e degli armadi separati e chiusi). Il trattamento di dati particolari o giudiziari dovrà infine prevedere l'utilizzo di appositi contenitori con lucchetti o serrature e definire una procedura di gestione delle chiavi. Inoltre, per il trattamento di dati particolari o giudiziari come definiti agli articoli 9 e 10 del Regolamento (UE) 2016/679, il responsabile deve assicurare che gli accessi a tali dati siano riservati al personale autorizzato e che il trasferimento dei documenti contenenti tali tipologie di dati avvenga in maniera cifrata.

È fatto comunque divieto al responsabile della diffusione dei dati, della comunicazione non autorizzata a Terzi e più in generale è fatto divieto di effettuare trattamenti non finalizzati all'esecuzione delle attività affidate, salvo a fronte di specifica autorizzazione da parte del titolare.

Le operazioni di trattamento devono essere gestite dal responsabile del trattamento in aderenza alle attività svolte nell'ambito dei progetti assegnati e in considerazione di eventuali e successive modifiche alle operazioni e/o modalità di trattamento apportate dal titolare, tramite integrazione delle presenti istruzioni.

Il responsabile è tenuto a mettere a disposizione del titolare tutte le informazioni necessarie all'espletamento delle attività di revisione, comprese le ispezioni, richieste dallo stesso titolare o da altro soggetto da esso autorizzato, al fine di rilevare il rispetto degli obblighi previsti dalla normativa vigente e dal presente accordo contrattuale.

Il Responsabile, ai sensi dell'art. 30 del Regolamento (UE) 2016/679, è tenuto a fornire al Titolare le informazioni necessarie alla compilazione del "Registro dei trattamenti". Qualora il Titolare intenda redigere la Valutazione di impatto prevista dall'art. 35 del Regolamento predetto, il Responsabile sarà tenuto a fornire anche le ulteriori informazioni che si rendessero necessarie alla redazione del documento.

Il Responsabile, qualora in ottemperanza all'obbligo di Legge, fosse tenuto ad individuare all'interno della propria organizzazione la figura del "Responsabile per la protezione dei dati personali", quest'ultimo sarà tenuto a svolgere la propria attività in stretta collaborazione con il Titolare. Il Responsabile deve procedere ad un controllo periodico sui rischi effettivi e sulla efficacia delle contromisure adottate, e deve redigere, in aggiunta al suindicato registro dei trattamenti, un documento che descriva le misure di sicurezza effettivamente adottate a fronte dei trattamenti assegnati ed ai requisiti sopra esposti.

Il Responsabile collaborerà attivamente con l'Autorità Garante per la Protezione dei dati personali e le Autorità Pubbliche, al fine di consentire a queste ultime l'esercizio delle proprie attività istituzionali, quali richieste di informazioni, attività di controllo mediante accessi ed ispezioni, relativamente ai trattamenti oggetto dell'Atto di nomina.