DATA PROTECTION AGREEMENT

ex art. 28 del Regolamento Europeo 679/2016

(Regolamento 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)

Con l'affidamento delle attività oggetto del presente contratto il CSI Piemonte (di seguito indicato come *Committente*), quale Titolare o come Responsabile di un trattamento di dati personali svolto per conto dei suoi Enti Clienti, affida all'Appaltatore il relativo trattamento di dati personali e/o sensibili (o particolari) e/o giudiziari.

Con il presente Data Protection Agreement (DPA), l'Appaltatore assume il ruolo di *Responsabile del trattamento* e si impegna ad effettuare, per conto del Committente, le operazioni di trattamento di seguito definite, nel rispetto del Regolamento Europeo 679/2016 (di seguito anche solo "GDPR") e del D. Lgs. 196/03 e s.m.i "*Codice in materia di protezione dei dati personali"* così come successivamente modificato ed integrato (di seguito anche solo "Codice").

In particolare, le Parti si impegnano a garantire il rispetto dei vincoli contenuti nell'articolo 28, paragrafi 3 e 4, del GDPR, e nelle "*Clausole contrattuali tipo tra titolari del trattamento e responsabili del trattamento*" emanate con Decisione di Esecuzione (UE) 2021/915 dalla Commissione Europea il 4 giugno 2021.

L'art. 28 comma 1 del GDPR attribuisce al Titolare del trattamento la facoltà di ricorrere ad un Responsabile che presenti, per esperienza, capacità ed affidabilità garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti previsti dalle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza e garantisca la tutela dei diritti dell'interessato. In virtù di tale prescrizione, il Responsabile adotta le misure tecniche ed organizzative di sicurezza dei dati personali e particolari, adeguate e specifiche alla/e tipologia/e di trattamento e già indicate nella tabella qui allegata, nonché le ulteriori misure migliorative eventualmente indicate nell'offerta tecnica presentata e/o nella documentazione prodotta.

I dettagli del trattamento sono di seguito specificati ("Trattamento di dati personali dei lavoratori" (cod. 001) del Registro dei Trattamenti del CSI Piemonte):

- **ambito di riferimento:** Gestione dele risorse umane
- **titolari del trattamento:** CSI Piemonte
- **tipo di dati personali**:
  - dati anagrafici e titoli di studio;
  - attività svolte e/o progetti seguiti, (compresi i Clienti interessati) e relativi dati economici e/o effort impiegato;
  - competenze professionali possedute;
  - percorsi di formazione fruiti;
  - profili professionali e collocazione negli anni entro l'organigramma aziendale;
  - elementi retributivi e/o di inquadramento contrattuale.
- **categorie di interessati:** Dipendenti

- **natura e finalità del trattamento:** i dati vengono trattati al fine di supportare il CSI a gestire il proprio personale con una modalità digitale, collaborativa, agile, basata sulle competenze e anche coerente con esperienze di lavoro dinamiche.

Nell'ambito del perimetro di trattamento suindicato, il Responsabile del trattamento dei dati personali si impegna a:

1) attenersi alle disposizioni previste dal Codice e dal GDPR ed operare nel rispetto dei principi espressi dalle norme in materia di trattamento di dati personali, sensibili (o particolari) e giudiziari, e in particolare dei principi di protezione dei dati sin dalla fase di progettazione e per impostazione predefinita (cd. *Privacy by design & by default*). Deve inoltre attenersi a tutte le prescrizioni previste - qualora ne ricorrano i presupposti - dai provvedimenti vigenti a carattere generale emanati dal Garante per la protezione dei dati personali, ed in particolare al Provvedimento relativo all'interscambio dei dati fra amministrazioni pubbliche del 2 luglio 2015, a quello sulle funzioni degli Amministratori di Sistema del 27 novembre 2008, laddove applicabili. Inoltre, qualora le mansioni oggetto del contratto richiedano competenze riconducibili a quelle degli Amministratori di Sistema, il Responsabile del trattamento dovrà fornire al Committente, nella persona del DEC, l'elenco delle persone fisiche designate ed il relativo ambito di responsabilità assegnata, all'avvio delle attività, dando notizia al medesimo Committente, nella persona del DEC, di tutte le eventuali modifiche e/o integrazioni che dovessero rendersi necessarie a tale elenco;

2) svolgere le attività di trattamento dati, secondo le istruzioni del Committente, eccezion fatta per i casi in cui una norma di legge cui è soggetto il Responsabile prescriva in modo difforme. In tal caso, il Responsabile informa il Committente circa tale obbligo giuridico prima del trattamento, a meno che la norma di legge applicata non lo consenta al fine di tutelare rilevanti motivi di interesse pubblico. Il Committente può impartire istruzioni successive per tutta la durata del trattamento dei dati personali. Tali istruzioni sono sempre documentate;

3) informare immediatamente il Committente qualora, a suo parere, le istruzioni ricevute violino il GDPR, il Codice o altre disposizioni applicabili, nazionali o europee, relative alla protezione dei dati;

4) adottare le misure tecniche ed organizzative di sicurezza dei dati personali e particolari adeguate alla/e tipologia/e di trattamento e indicate nella tabella qui allegata nonché le ulteriori misure migliorative eventualmente indicate nell'offerta tecnica presentata. 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. Nel valutare l'adeguato livello di sicurezza, le Parti hanno tenuto 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. Le misure devono in ogni caso essere conformi alle indicazioni o best practices (tra cui, a titolo meramente esemplificativo, le linee guida AGID circa le "Misure minime di sicurezza ICT per le pubbliche amministrazioni", e le "Linee guida AGID per lo sviluppo del software sicuro").

Nel corso della durata del contratto, dette misure possono essere integrate o riviste nei seguenti casi:

- a seguito di un'eventuale revisione dell'analisi dei rischi sul trattamento dei dati;
- in occasione del vulnerability assessment periodico, qualora l'affidamento abbia ad oggetto una soluzione informatica;
- a seguito di un aggiornamento normativo o regolamentare.

In ogni caso l'elenco delle nuove misure, condivise formalmente con il Committente, costituiscono integrazioni al contratto in essere tra le Parti.

5) consentire l'accesso ai dati personali unicamente alle persone fisiche autorizzate, e solo dopo aver fornito ad esse tutte le istruzioni sufficienti e necessarie ad eseguire il trattamento in base alle istruzioni fornite dal titolare o dal Committente per conto del titolare, ai sensi dell'art. 29 del GDPR, e solo nella misura strettamente necessaria per l'attuazione e la gestione delle attività oggetto del presente contratto; a garantire che gli stessi soggetti si siano impegnati a rispettare gli obblighi di segretezza e riservatezza previsti e abbiano ricevuto la formazione necessaria e le istruzioni dettagliate finalizzate a trattare in modo sicuro e riservato i dati affidati, custodendoli e controllandoli nel modo più appropriato. Su richiesta del Committente, il Responsabile nel corso della durata del contratto deve fornire evidenze della formazione erogata in materia di protezione dei dati personali e/o delle istruzioni fornite alle risorse impiegate nei servizi oggetto dell'appalto in ottemperanza agli obblighi previsti dal GDPR. Se il trattamento riguarda dati particolari ai sensi degli artt. 9 e 10 del GDPR, il Responsabile applica ulteriori limitazioni specifiche e/o garanzie supplementari;

6) redigere il registro delle attività di trattamento in conformità ai requisiti previsti all'art. 30 comma 2 del GDPR con i trattamenti svolti per conto del Committente;

7) non trasferire tutti o alcuni dati personali trattati verso un paese terzo o un'organizzazione internazionale, se non su istruzione documentata del Committente o previa autorizzazione dello stesso e fornendo, in tale ultimo caso, indicazioni della base legale che legittima il trasferimento in conformità a quanto previsto nel capo V del GDPR;

8) comunicare al DEC ogni ricorso a sub-Responsabili cui devono essere affidate specifiche attività che comportano un trattamento di dati personali, con un anticipo di almeno 20 gg al fine di consentire l'esercizio del diritto di opposizione del Titolare in conformità all'art. 28 comma 2 del GDPR. Tale comunicazione scritta, che contiene ogni informazione utile ed in particolare, denominazione, sede ed attività affidata, dovrà essere formalizzata anche nel corso della durata del presente contratto per ogni modifica o integrazione dei sub-Responsabili del trattamento.

Il Responsabile si impegna in ogni caso a selezionare i sub-responsabili tra soggetti che per esperienza, capacità e affidabilità forniscano garanzie sufficienti in merito a trattamenti effettuati in applicazione della normativa pro tempore vigente e che garantiscano la tutela dei diritti degli interessati. Si impegna altresì a far sottoscrivere copia delle presenti clausole (comprese le misure tecniche ed organizzative di sicurezza) o stipulare specifici atti in cui siano descritti analiticamente i compiti assegnati a detti sub-Responsabili che prevedano l'obbligo di pieno rispetto dei medesimi adempimenti in materia di protezione dei dati personali derivanti dalle presenti clausole.
Il Responsabile del trattamento rimane comunque pienamente responsabile dell'adempimento degli obblighi da parte dei sub-Responsabili, e notifica al Committente qualunque

loro inadempimento e si impegna a fornire, se richiesto, copia del contratto stipulato con il sub-Responsabile e di ogni successiva modifica.
Il Responsabile si impegna a formalizzare con il sub-Responsabile una clausola a favore del Committente in base alla quale, qualora il Responsabile abbia giuridicamente cessato di esistere o siano in corso nei suoi confronti procedimenti di accertamento dello stato di crisi o insolvenza, il Committente ha il diritto di imporre al sub-Responsabile di cancellare o restituire i dati personali trattati per conto del Committente;

9) tenendo conto delle informazioni a sua disposizione e delle istruzioni ricevute, coadiuvare ed assistere il Committente e/o il Titolare nelle attività svolte, ed in particolare a garantire:

- ✓ il rispetto dei principi di esattezza e aggiornamento dei dati: il Responsabile informa senza indugio il Committente qualora venga a conoscenza del fatto che i dati che sta trattando sono inesatti o obsoleti;
- ✓ l'esercizio dei diritti degli interessati di cui agli artt. da 12 a 22 del GDPR, notificando prontamente al Committente qualunque richiesta ricevuta dall'interessato: il Responsabile non risponde alla richiesta a meno che sia stato autorizzato in tal senso dal Committente;
- ✓ la redazione o l'aggiornamento della valutazione d'impatto sulla protezione dei dati, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, fornendo eventualmente le informazioni o la documentazione necessaria (es. analisi dei rischi);
- ✓ la necessità di consultare - prima di procedere al trattamento – l'Autorità Garante per la protezione dei dati personali qualora la valutazione di impatto indichi che il trattamento presenti ancora un rischio elevato nonostante le misure adottate dal Titolare per mitigare il rischio;

10) in caso di violazioni di dati personali, cooperare nell'adempimento degli obblighi previsti dagli artt. 33 e 34 del GDPR in capo al Titolare, tenuto conto della natura del trattamento e delle informazioni a disposizione. In particolare, in caso di violazione di dati trattati dal Responsabile, lo stesso notifica al Committente senza ingiustificato ritardo dopo esserne venuto a conoscenza, le seguenti informazioni:

- ✓ una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
- ✓ i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
- ✓ 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.

Nel caso di violazione dei dati trattati dal Committente e/o dal Titolare, se richiesto, il Responsabile fornisce assistenza nel notificare la violazione dei dati al Garante per la

protezione dei dati personali per fornire le informazioni che devono essere indicate nella notifica.

11) rispondere prontamente ed adeguatamente alle richieste di informazioni del Committente fornendo tutte le informazioni e mettendo a disposizione la documentazione necessaria al fine di dimostrare il rispetto degli obblighi previsti dal Codice e dal GDPR.
Il Responsabile deve inoltre consentire al Committente, a intervalli ragionevoli, attività di ispezione, audit o riesame delle attività senza costi aggiuntivi per il Committente. A tal fine, il Committente può tenere conto delle pertinenti certificazioni in possesso del Responsabile e può scegliere di condurre l'attività di verifica autonomamente o incaricare un revisore indipendente. Le attività di verifica possono comprendere anche ispezioni nei locali o nelle strutture fisiche del Responsabile e, se del caso, devono essere effettuate con un preavviso ragionevole. Su richiesta, le Parti mettono a disposizione delle autorità competenti le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di verifica;

12) per quanto di competenza, prestare tutta la collaborazione necessaria a fronte di richieste di informazioni, controlli, ispezioni ed accessi da parte dell'Autorità Garante o di altre pubbliche Autorità competenti (informando contestualmente il Committente con la massima celerità);

13) in caso di contestazione di una violazione degli obblighi di cui sopra e su richiesta del Committente, sospendere immediatamente il trattamento dei dati personali a cui tale contestazione si riferisce e ad informare prontamente il Committente in merito al fatto di essere in grado o meno di rispettare gli obblighi richiesti, al fine di consentire al Committente di intraprendere, entro un termine ragionevole, le misure necessarie, a tutela del trattamento dei dati;

14) al termine del trattamento, o in ogni altro caso di cessazione del trattamento, restituire al Committente o cancellare i dati del Titolare sulla base delle istruzioni ricevute e senza ulteriori oneri, certificandone la cancellazione delle copie, fatto salvo il caso in cui una norma di legge non ne preveda la conservazione.

Il Responsabile comunica al Committente il nome e i dati di contatto del proprio Responsabile per la Protezione dei dati, qualora ne abbia designato uno conformemente all'art. 37 del GDPR e si impegna, qualora, nel corso di vigenza del contratto, intervengano variazioni, a darne pronta comunicazione al Committente.

MISURE TECNICHE ED ORGANIZZATIVE

Misure di sicurezza organizzative:

misura	descrizione/esempi
Definizione del modello organizzativo	Sono definite regole e responsabilità a livello aziendale e nell'ambito dell'attività affidata in materia di sicurezza e privacy e a livello di ruoli e responsabilità (es codice etico, profili professionali, regolamento privacy)
Formazione e sensibilizzazione del personale	È definito un piano di formazione in materia di protezione dei dati per il trattamento. Sono stati eseguiti gli interventi formativi previsti dal piano
Istruzioni per il trattamento	Sono definite e diffuse al personale interno le istruzioni per l'esecuzione del trattamento (principi, regole da applicare nel trattamento, procedure, linee guida, manuali di organizzazione del servizio, gestione degli archivi cartacei, gestione dei supporti ecc..) Sono definite le procedure/istruzioni di lavoro per la gestione degli incidenti che possano comportare violazione di dati personali (data breach)
Audit	Viene effettuata un'attività di audit che include controlli nell'ambito della protezione dei dati personali
Regolamentazione misure applicate nei rapporti con i fornitori	I contratti che il fornitore stipula con eventuali sub fornitori che operano sul trattamento includono ~~le~~ clausole privacy per il rispetto del GDPR. Sono definite eventuali clausole e condizioni di dettaglio specifiche per il trattamento
Predisposizione di un modello per l'analisi dei rischi di privacy/sicurezza e PBDD	È adottato un modello per l'analisi, la valutazione e il trattamento dei rischi di sicurezza e privacy e un modello per documentare l'applicazione dei principi di privacy by design e by default (PBDD)
Documentazione del software e del servizio	Sono predisposti e aggiornati i documenti di progettazione, architettura, installazione del software utilizzato (es vista d'insieme, documento di architettura, deploy, ..) e per la gestione del servizio

Misure di sicurezza tecniche trasversali:

Misura	descrizione/esempi
Antivirus	Sulle postazioni di lavoro sono installati antivirus aggiornati quotidianamente
Gestione delle postazioni di lavoro	Sono adottate misure per ridurre la possibilità che le postazioni di lavoro (sistemi operativi, applicazioni aziendali, software per ufficio, impostazioni etc.) vengano sfruttate per violare la sicurezza dei dati con particolare riferimento a quelli personali
Protezione della navigazione web (web filtering)	Si adottano policy/regolamenti e/o sistemi di navigazione protetta per evitare l'accesso a risorse web non autorizzate o che possano essere veicolo di minacce
Misure antincendio	L'edificio in cui sono conservati i dati è dotato di misure antincendio di protezione dei beni e dei documenti
Sistemi di sorveglianza	L'edificio in cui sono conservati i dati è dotato di misure di controllo accessi ai locali e di videosorveglianza
Utilizzo di infrastrutture sicure (hw e complementari)	Le infrastrutture hardware e i sistemi complementari sono manutenuti e aggiornati regolarmente e rispettano i requisiti minimi di sicurezza AgID
Infrastrutture logiche aggiornate	Le infrastrutture software (es. middleware, software dei sistemi, ..) sono costantemente aggiornate
Network monitoring	Si utilizzano strumenti di monitoraggio del traffico di rete (es. IDP, packet filtering, …) volti ad individuare situazioni anomale o malevole
Separazione LAN	L'infrastruttura LAN utilizzata per le attività adotta la separazione tra ambienti sviluppo, test, collaudo e produzione
Accessi da remoto con VPN	Si utilizza il sistema/protocollo VPN o altri strumenti per l'accesso alle risorse da remoto sui server del fornitore (da parte di dipendenti o terzi)
Protezione perimetrale (firewall)	vengono utilizzati strumenti di protezione della rete (es. firewall, misure anti DDos, WAF)
Gestione Log accessi privilegiati	Si utilizzano strumenti per la gestione dei log dei sistemi (es log dei server dei database, dei firewall, ecc..). I log generati vengono esaminati per rilevare e gestire eventi di sicurezza
Backup	Sono disponibili servizi infrastrutturali di backup

Ulteriori misure tecniche di sicurezza applicate:

Misura	descrizione/esempi
Gestione delle credenziali	Ogni autorizzato è dotato di credenziali individuali e di un profilo che consente il solo trattamento dei dati necessari per l'attività (es. per l'accesso a database, la connessione VPN verso infrastruttura CSI, l'autenticazione ad applicativi software). Le credenziali vengono disattivate da CSI quando l'autorizzato non effettua più attività di trattamento, pertanto il fornitore adotta un processo di segnalazione delle variazioni

misura	descrizione/esempi
Minimizzazione della quantità dei dati personali	Nel trattamento sono adottate misure per ridurre la quantità dei dati necessari quali tecniche di filtraggio e rimozione, riduzione della sensibilità attraverso la conversione, riduzione della natura identificativa del dato, riduzione dell'accumulazione, limitazione dell'accesso
Autorizzazione	Sono utilizzati sistemi di gestione delle autorizzazioni con un grado di sicurezza adeguato in relazione al trattamento (es sistemi di autorizzazioni centralizzati con adeguato livello di sicurezza in relazione all'esigenza del trattamento)
Autenticazione	Si utilizza un sistema di autenticazione (locale o nazionale) con un grado di sicurezza adeguato in relazione al trattamento
Gestione del ciclo di vita delle credenziali	È garantita la gestione del provisioning e deprovisioning delle credenziali di autenticazione e della profilazione (creazione, revoca, modifica di credenziali di autenticazione e di informazioni di profilazione) in particolare della scadenza della credenziale (anche in termini di gestione delle segnalazioni da sistemi centralizzati)
Tracciabilità accessi risorse	È garantita la possibilità di tracciare accessi alle risorse critiche impiegate nel trattamento (es database, front end e back end del servizio, share di rete). Il controllo può ad esempio essere implementato per un database, andando a garantire la tracciatura dell'identificativo dell'utente che ha inserito/modificato/cancellato i dati della tabella
Audit log applicativi	L'applicazione software traccia mediante log operazioni significative compiute dagli utenti su dati personali
Minimizzazione della vulnerabilità delle risorse utilizzate nel trattamento	Sono previste opportune tecniche per ridurre la vulnerabilità delle risorse impiegate nel trattamento (es politiche di aggiornamento del software, test funzionale e di vulnerabilità del software utilizzato da aggiornare periodicamente, limitazioni dell'accesso fisico al materiale che contiene dati personali)
Cifratura del dato	Sono adottati opportuni mezzi per cifrare i dati (in database, file, backup etc.), così come le procedure per gestire chiavi crittografiche (creazione,

	archiviazione, aggiornamento in caso di compromissione etc.)
Cifratura del canale	Viene utilizzato un canale cifrato per le comunicazioni mediante l'impiego di protocolli sicuri (es. HTTPS e SSH)
Pseudonimizzazione	Sono adottate tecniche che garantiscono la non attribuzione a una persona identificata o identificabile di un dato ma consentono di identificare in un secondo momento i dati anche in maniera indiretta o da remoto (es conservando separatamente le informazioni che permettono di associare la persona al dato)
Backup cifrati	Sono utilizzati sistemi per la cifratura dei backup