Allegato alla Lettera di invito
Check - List Privacy by design

Al fine di garantire i requisiti di privacy by design, ai sensi dell'articolo 25 del Regolamento (UE) 2016/679, Pensplan Centrum S.p.A. richiede apposite garanzie e funzionalità agli operatori economici partecipanti alla procedura di affidamento, laddove il servizio/fornitura implichi il trattamento di dati personali. Per tale ragione, la Check-List per la Privacy by design qui di seguito riportata rappresenta un documento integrante la documentazione di gara. Si richiede all'operatore economico la compilazione della predetta Check-List, di modo da fornire, nella fase di valutazione dell'offerta e prima della stipula del contratto, le informazioni utili anche al fine di procedere alle analisi necessarie all'avvio dell'eventuale procedura di valutazione d'impatto sulla protezione dei Dati/Data Protection Impact Assessment (DPIA).

Inserire Nome Operatore Economico		
MISURE DI SICUREZZA	**(SI/NO/NA)**	**Note (eventuali osservazioni/precisazioni)**
1. L'operatore economico ha adottato o definito politiche/policy e procedure interne sulla sicurezza delle informazioni, dei sistemi e dei dati personali.		
2. Queste policy sono contenute in specifici documenti resi disponibili anche al personale.		
3. Tali documenti sono oggetto di revisione periodica.		
4. L'operatore economico ha individuato il personale autorizzato al trattamento dei dati personali mediante apposita comunicazione.		
5. Sono impartite istruzioni sulle misure di sicurezza al personale autorizzato al trattamento dei dati personali anche in relazione agli obblighi di riservatezza.		I
6. Sono previsti corsi di formazione per il personale autorizzato al trattamento.		

7. Sono impartite istruzioni sulle misure di sicurezza al personale autorizzato (es.: addetti IT) di fornitori od outsourcer (responsabili del trattamento) operanti presso la Società.		I
8. Sono designate le persone a cui sono attribuiti privilegi informatici o funzioni di Amministratori di sistema (ADS), previa valutazione dei loro requisiti, ed adottate le correlate misure organizzative e tecniche indicate dal Garante privacy.		
9. Gli accessi sia al software sia ai dati sono controllati da sistemi di autenticazione. Ogni utente accede solo ai dati di propria competenza		
10. L'accesso ai sistemi operativi, reti, servizi IT, applicazioni, sistemi, software, database e ai dati personali avviene attraverso una procedura di autenticazione degli utenti che prevede l'inserimento delle relative credenziali. Il mancato inserimento oppure l'inserimento errato delle credenziali di autenticazione non consente in nessun caso l'accesso. Tutti i sistemi, come impostazione predefinita, sono predisposti per negare l'autorizzazione dell'accesso a qualsiasi persona.		
11. Le credenziali di accesso attivate sono individuali e sempre corrispondenti ad un'identità univoca.		
12. L'accesso alle funzioni dei sistemi ed ai dati in essi trattabili è limitato in base alle autorizzazioni/abilitazioni assegnate.		
13. Specifiche funzionalità dei sistemi che consentono un trattamento massivo di dati sono accessibili solamente da parte del personale del reparto tecnico informatico		
14. Gli accessi sono gestiti con procedure di login sicure, mediante l'inserimento di una username e di una password.		
15. In tutti i sistemi è previsto l'oscuramento delle password al momento della digitazione.		

16. I criteri di complessità minima delle password sono definiti in almeno 8 caratteri.		
17. I nuovi account sono configurati sulla base di privilegi associati a profili autorizzativi predeterminati. I profili autorizzativi predeterminati consentono l'accesso esclusivamente ai sistemi necessari per l'espletamento delle mansioni previste in relazione all'utilizzo delle apparecchiature (postazione di lavoro) e alle risorse di rete (file-sharing, internet, ecc.).		
18. Gli account ed i profili in questione sono disattivati o modificati in caso di cessazione dei rapporti di lavoro o di variazione dell'ufficio o dei compiti assegnati alle persone autorizzate, su segnalazione ad esempio del reparto Risorse Umane al reparto tecnico informatico.		
19. I diritti di accesso degli utenti sono riesaminati periodicamente e sempre a seguito di ogni modifica contrattuale (es. promozioni, nuovi incarichi, altro). Inoltre vengono modificati ed assegnati in base alle necessità operative sulla base di quanto definito e preventivamente autorizzato dalla struttura competente.		
20. A seguito di eventuali richieste di ripristino/reset di password, per smarrimento o sospetta compromissione, il personale tecnico informatico verifica l'identità dell'utente a cui si riferisce la richiesta, contattandolo direttamente e confermando la consapevolezza circa la richiesta pervenuta.		
21. Le credenziali di accesso sono comunicate al personale autorizzato dagli addetti del reparto tecnico informatico con le seguenti modalità: verbalmente in caso di impossibilità di accesso ai sistemi, per iscritto o mediante strumenti telematici.		

22. A tutti gli utenti viene assegnata una username ed una password predefinita, in base ad una combinazione di caratteri alfanumerici secondo i criteri di complessità minima definiti.		
23. La password deve essere sostituita almeno ogni 60 giorni.		
24. Le istruzioni e responsabilità degli utenti circa l'utilizzo delle credenziali di autenticazione sono definite nel Regolamento interno per il trattamento dei dati personali e l'uso degli strumenti di lavoro (comunicato o reso conoscibile a tutto il personale).		
25. Sono presenti sistemi che verificano costantemente eventuali malfunzionamenti o degradi di performance della rete informatica e sistemi che verificano costantemente eventuali accessi di apparecchiature non aziendali alla rete informatica.		
26. Sono implementate misure di sicurezza a livello perimetrale tramite opportuni strumenti (es. firewall e IDS/IPS) al fine di filtrare il traffico anomalo e prevenire, laddove possibile, attacchi dall'esterno o da parte di soggetti interni non autorizzati.		
27. Sono presenti apparecchiature (Firewall, Antispam) che effettuano un controllo costante di tutte le comunicazioni da e per la rete aziendale, verificandone sia il valido contenuto (eventuali virus) sia la corretta destinazione/provenienza.		
28. L'accesso a Internet e alle email è opportunamente verificato e protetto tramite meccanismi di Web/URL filtering ed Email Security/Antispam al fine di impedire l'accesso a siti web o servizi considerati non sicuri e la ricezione di email malevole, di phishing o spam.		
29. Sono presenti sistemi centralizzati per la gestione dei programmi Antivirus. Le "firme" delle basi virali sono aggiornate ogni ora.		

30. Tutti i sistemi client e server sono protetti da virus, malware e agenti malevoli tramite l'adozione di soluzioni antivirus costantemente aggiornate ed è reso impossibile modificare/disabilitare le soluzioni di protezione agli utenti che accedono ai sistemi.		
31. Gli accessi ai sistemi o ai dati personali effettuati dal personale autorizzato sono tracciati in appositi log che sono conservati per periodi di tempo necessari alla verifica di eventuali anomalie.		
32. Gli accessi ai sistemi con utenze con privilegi speciali (es. utenze amministrative, come i c.d. Amministratori di Sistema - ADS) sono opportunamente tracciati in appositi log che sono conservati per i tempi previsti dal Garante privacy.		
33. Sono definiti opportuni processi e strumenti di monitoraggio al fine di identificare, analizzare e classificare eventi anomali in termini di sicurezza in funzione del loro livello di criticità o potenziali attacchi interni ed esterni (es. Data Breach) monitorandone l'evoluzione fino alla loro effettiva risoluzione.		
34. Sono definite procedure per la gestione e notifica di eventuali violazioni di dati personali (Data Breach) e loro comunicazione agli interessati, ove necessario.		
35. Sono fornite opportune indicazioni al personale affinché provveda a segnalare tempestivamente, alle strutture preposte e secondo le procedure definite, eventuali problematiche di sicurezza e Data Breach.		
36. E' prevista una verifica periodica degli alert generati dal sistema con funzionalità di analisi dei log, che segnala tentativi di violazione delle regole definite per un utilizzo accettabile dei servizi e sistemi informatici.		

37. Il personale tecnico informatico utilizza appositi ambienti di sviluppo (server, ambienti applicativi, etc.) prima della messa in produzione di nuove procedure e/o applicazioni.		
38. Lo sviluppo di software avviene su macchine aziendali che utilizzano database non in produzione.		
39. In questi ambienti di sviluppo si effettuano test e simulazioni utilizzando dati di test modificati ad hoc.		
40. Gli ambienti di sviluppo e test sono accessibili solo al personale tecnico informatico e ad utenti specifici.		
41. Costantemente è verificato che gli ambienti di test e di sviluppo siano correttamente utilizzati e configurati. Inoltre è verificato che le regole di migrazione dall'ambiente di sviluppo a quello di produzione siano aggiornate e rispettate. Ad ogni migrazione dall'ambiente di test verso l'ambiente di produzione è verificato infine che le utenze e le password utilizzate non vengano trasferite.		
42. Sono adottate misure di pseudonimizzazione e cifratura dei dati personali, in relazione ad attività di trattamento che risultano rischiose od altamente rischiose – es.: trattamenti di dati particolari (es: sanitari, biometrici), attività automatizzate di profilazione dei clienti e processi decisionali automatizzati; banche dati di rilevanti dimensioni o trattamenti su larga scala, ecc.		
43. E' possibile, in relazione ai tempi di conservazione dei dati personali definiti internamente, eseguire le operazioni di cancellazione dei dati allo scadere dei termini fissati dalle strutture dell'Operatore economico.		
44. Nei casi di trattamento di dati personali per i quali sia applicabile il diritto alla portabilità, sono previsti programmi o procedure che, ove l'interessato lo richieda, permettono di estrarre una copia dei dati in un formato aperto/interoperabile da fornire al medesimo interessato o da comunicare ad altro titolare del trattamento da lui indicato.		

45. Gli interventi di aggiornamento della console vengono effettuati dal personale del reparto tecnico informatico. La distribuzione degli aggiornamenti sui singoli terminali avviene automaticamente ad ogni nuovo rilascio.		
46. Sono effettuati con cadenza periodica (semestrale/annuale) gli aggiornamenti dei programmi software, applicativi e servizi informatici al fine di prevenire eventuali vulnerabilità e correggere eventuali difetti.		
47. Sono utilizzati protocolli crittografici di comunicazione (es. SFTP, HTTPS, ecc.), in fase di accesso a portali web e/o scambio di file, agli strumenti IT gestiti dall'Operatore economico ed esposti all'esterno su rete internet oppure agli strumenti di terze parti utilizzati per lo scambio di informazioni tra l'Operatore economico ed alcuni responsabili esterni del trattamento.		
48. E' prevista una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.		
49. Periodicamente vengono effettuati dei penetration test per prevenire eventuali rischi di intrusione. Gli sviluppatori seguono regole specifiche di programmazione per ridurre i rischi d'intrusione attraverso applicativi webbased.		
50. Sono definite procedure di backup periodiche finalizzate a garantire la disponibilità dei dati, la possibilità di ripristino in caso di eventi dannosi e questi sono conservati in modalità sicura, limitandone l'accesso al solo personale autorizzato.		
51. E' prevista la ripartenza delle attività quotidiane presso una sede alternativa. Tale ripartenza viene simulata e testata annualmente.		

52. E' effettuato, con cadenza periodica (per i dati di business, con cadenza giornaliera, per altre tipologie di dati, con cadenza bimensile), test di ripristino delle informazioni al fine verificare l'effettiva possibilità di recupero delle informazioni e dei dati del Titolare oggetto di backup.		
53. L'Operatore economico è dotato di un piano di Disaster Recovery volto a garantire la propria operatività anche in caso di eventi di grave criticità quali: indisponibilità dei locali; indisponibilità delle infrastrutture di erogazione dell'energia elettrica; indisponibilità dei sistemi informativi; etc.		
54. Il reimpiego, il riciclaggio o lo smaltimento degli strumenti elettronici (pc, dispositivi, supporti, ecc.) viene gestito attraverso fornitori esterni che si impegnano contrattualmente a gestire lo smaltimento secondo i requisiti di legge. La cancellazione sicura dei dati (es. formattazione) o la loro distruzione è effettuata dal reparto tecnico informatico.		
55. Sono previsti nell'ambito degli accordi o contratti con gli outsourcer o fornitori di servizi informatici/telematici specifici obblighi di adozione di adeguate misure organizzative e tecniche in materia di sicurezza dei sistemi e dati.		
56. L'accesso ai locali fisici dell'Operatore economico sono controllati da personale addetto al ricevimento di personale esterno. Tutti i locali contenenti dati sono chiusi a chiave e protetti da un sistema d'allarme. Ogni locale è protetto da un sistema di rilevazione fumo e dotato di estintori per la soppressione di focolai d'incendio.		
57. I locali tecnici e/o gli armadi tecnici sono dotati di sistemi d'allarme.		
58. I locali ospitanti i sistemi di business (es. server, dati) sono dotati di apposite misure di sicurezza fisica degli ambienti ed accesso alle infrastrutture tecnologiche mediante impianti antincendio, antintrusione, antifurto, videosorveglianza, nonché impianti di raffreddamento dei locali, ricambio dell'aria e impianti di spegnimento automatico. Tali locali rispettano le misure di sicurezza relative alle norme ISO 27001.		

59. L'Operatore economico ha ottenuto una certificazione in materia di sicurezza delle informazioni (es.: ISO 27001), dei sistemi o dei dati personali (art. 42 del GDPR).		
60. Le misure di sicurezza di alcuni sistemi sono presidiate direttamente dagli outsourcer/fornitori dell'Operatore economico che li gestiscono.		