UNIVERSITÀ di VERONA

CHECKLIST VALUTAZIONE DEL SERVIZIO

In qualità di nostro Responsabile del trattamento, Vi invitiamo a procedere alla compilazione e alla successiva trasmissione del seguente questionario per la valutazione nonché l'autovalutazione **della Vostra conformità, in quanto soggetto giuridico sottoposto alla vigente normativa in materia di protezione dei dati personali**. **La trasmissione dovrà avvenire 'brevi manu', oppure a mezzo posta elettronica certificata all'indirizzo: ufficio.protocollo@pec.univr.it, entro e non oltre 7 giorni dal ricevimento della presente, e comunque in tempo utile per la sottoscrizione o per il rinnovo del contratto di servizio.**
In alternativa e/o in aggiunta alla compilazione del presente questionario, è sempre possibile inviare alla Scrivente diversa documentazione attestante la propria compliance privacy (es. Procedura Valutazione Fornitori ISO 9001/27001, o ulteriore materiale messo a disposizione anche mediante il sito web).

Il questionario è compilato in data __/__/__ dal Sig./Sig.ra _____

per conto di _____

a) Si ricorda che per la corretta compilazione dovrà essere inserita una spunta in ciascuna delle voci, a seconda dello stato di implementazione della misura da voi implementata, evidenziando che è altresì richiesto obbligatoriamente, a titolo di trasparenza, riportare nelle note una breve descrizione delle valutazioni preventive adottate all'interno della Vostra organizzazione, tali da dimostrare la Vostra concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. La compilazione priva delle valutazioni preventive adottate non potrà essere considerata valida.

Denominazione servizio	
Tipologia servizio	☐ Software o sito web on premise c/o machine Ateneo ☐ Sito Web in hosting su macchine non dell'ateneo ☐ Saas ☐ IaaS ☐ PaaS ☐ Altro:
Fornitore	
Descrizione sintetica attività gestita	Descrizione ambito Operativo:
Tecnologia	
Modalità di erogazione	☐ On premise ☐ Hosting ☐ Cloud pubblico ☐ Cloud privato ☐ Cloud ibrido
Modalità di hosting/housing	
Banca dati	

UNIVERSITÀ di VERONA

COMPLIANCE SICUREZZA E PRIVACY DEL SERVIZIO

1. Compliance generale al Regolamento Generale sulla protezione dei dati 2016/679 (GDPR)

Il servizio è integrato con sistemi di sicurezza permettendo la conformità al GDPR necessarie per lo scenario d'impiego cui è destinato: Privacy by design; Privacy by default; minimizzazione; pseudonimizzazione, PET (Privacy Enhancing Technologies). O comunque, Il servizio è parzialmente integrato con sistemi di sicurezza, tuttavia è possibile sviluppare dei controlli compensativi che permettono la conformità al GDPR necessarie per lo scenario di impiego cui è destinato.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

2. Autenticazione e log

2.1 Il servizio permette l'autenticazione degli utenti basata su tecniche di strong authentication (autenticazione basata su password e MFA comeOTP, SPID, CIE ecc.), o tramite smart card (CNS, ecc.)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

2.2 Sono previste per default tecniche di abilitazione automatica di meccanismi di costruzione di password complesse (lunghezza almeno 12 caratteri)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

2.3 La componente privata delle credenziali di accesso è di almeno 8 caratteri

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

2.4 È prevista l'obbligatorietà del cambio password al primo accesso (in quanto compatibile con il sistema di autenticazione offerto)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

2.5 È prevista la modifica obbligatoria della password ogni 3 / 6 mesi (in quanto compatibile con il sistema di autenticazione offerto)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

2.6 È prevista la disattivazione automatica dell'accesso all'applicativo dopo 6 mesi di non utilizzo o altro tempo parametrizzabile

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	

	Implementato	
	Non applicabile	

2.7 Il servizio tiene traccia (log accessi e log attività) delle operazioni effettuate tramite applicativo (LOG APPLICATIVO), comprese le attività di sola visualizzazione dei dati, per un tempo parametrizzabile e adeguato a quanto previsto da norme di legge e/o regolamenti (es. 24 mesi per il dossier sanitario)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

2.8 Il servizio permette la profilazione degli utenti (dipendenti autorizzati ad istruire le pratiche e quindi al trattamento dei relativi dati personali) in modo granulare da consentire solo la visibilità dei dati necessari al ruolo svolto.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

3. Rispetto delle misure e degli accorgimenti in tema di amministratori di sistema (per la parte di competenza del fornitore)

3.1 È prevista la possibilità di creare livelli differenziati di amministrazione del sistema

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

3.2 È previsto un sistema di registrazione (access log) per gli accessi logici degli amministratori di sistema al database di supporto del servizio

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

3.3 Il sistema di access log ha caratteristiche di inalterabilità, completezza e di verifica della integrità dello stesso

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

3.3 L'access log contiene almeno i riferimenti temporali, la descrizione dell'evento che le ha generate, l'identificazione del soggetto che ha compiuto l'accesso

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

3.4 L'access log è conservato per almeno sei mesi o per il maggior tempo richiesto dalla normativa e/o da regolamenti (es. 24 mesi per il dossier sanitario)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	

	Implementato	
	Non applicabile	

4. Misure specifiche per categorie particolari di dati personali i dati personali relativi a condanne penali e reati

4.1 Le categorie particolari di dati personali (fra i quali rientrano ad es. i dati idonei a rivelare lo stato di salute, o la vita sessuale/orientamento sessuale), e/o i dati personali relativi a condanne penali o reati, sono registrati e conservati separatamente dagli altri dati personali soggetti a trattamenti. (DISACCOPPIAMENTO)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

4.2 Le categorie particolari di dati personali (fra i quali rientrano ad es. i dati idonei a rivelare lo stato di salute, o la vita sessuale/orientamento sessuale), o i dati personali relativi a condanne penali o reati sono gestiti mediante tecniche di CIFRATURA.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

4.3 Il servizio prevede tecniche di PSEUDONIMIZZAZIONE in relazione alla gestione di categorie particolari di dati personali, e/o dati personali relativi a condanne penali o reati

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

4.4 Le categorie particolari di dati personali, e/o i dati personali relativi a condanne penali o reati, sono trattati mediante CODICI IDENTIFICATIVI che non esplicitano direttamente il contenuto informativo

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

4.5 Le categorie particolari di dati personali, e/o i dati personali relativi a condanne penali o reati, sono trattati mediante ALTRE SOLUZIONI rispetto alle precedenti, ai fini della loro temporanea inintelligibilità (Se SI descriverle in tabella)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

4.6 I documenti che contengono in modo non divisibile dati personali, e categorie particolari di dati personali e/o i dati personali relativi a condanne penali o reati, sono trattati mediante tecniche di cifratura

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

5. Cancellazine dei dati

5.1 Il sistema consente di definire, per classi di informazioni, il tempo di conservazione in relazione al momento in cui sono state prodotte e al momento in cui è stata raggiunta la finalità per le quali sono state raccolte.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

5.2 Il sistema consente la cancellazione delle informazioni che hanno raggiunto il tempo limite di conservazione

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

5.3 Il sistema consente di individuare le informazioni relative ad un soggetto (interessato) e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

5.4 Il sistema dispone di servizi (esempio in collaborazione applicativa) che consentono ad un sistema esterno di individuare le informazioni relative ad un soggetto (interessato) e in modo puntuale settarle per la cancellazione, il blocco, e l'eventuale ripristino a seguito di blocco

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6. Misure di dispiegamento

6.1 Il servizio prevede la gestione aziendale/multi-aziendale con i dati su db criptato

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.2 Il servizio prevede la gestione multi-aziendale con separazione fisica dei dati di ciascuna azienda

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.3 Il servizio prevede la gestione multi-aziendale con separazione logica dei dati di ciascuna azienda (Se SI descrivere in tabella la tecnica utilizzata)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.4 Il servizio supporta protocolli di comunicazione sicuri e cifrati (HTTPS, SSH v2, ecc.)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.5 Il livello di Amministratore DBA consente di attribuire separatamente le competenze sulla base anagrafica da quelle sulle categorie di Dati Particolari e/o dati personali relativi a condanne penali o reati

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.6 Il livello di Amministratore DBA consente di attribuire separatamente le competenze sui dati di una Azienda rispetto ai dati di un'altra Azienda gestite nello stesso impianto

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.7 L'architettura del software, del db e dei servizi utilizzati consente un dispiegamento su due o più nodi in HA

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.8 L'architettura del software, del db e dei servizi utilizzati consente un dispiegamento su due o più nodi in modalità attivo-attivo su LAN geografica

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.9 È garantita l'indipendenza da figure chiave di amministrazione/gestione, senza le quali non è assicurata l'operatività (ridondanza adeguata delle figure strategiche)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.10 È effettuata la ricerca continua delle vulnerabilità sia sul codice che sulla configurazione e sono eseguiti penetration test applicativi prima del passaggio in produzione

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

6.11 Il servizio è adeguato alle Linee Guida AgID (Misure Minime, Sviluppo del software sicuro, etc.)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	

	Implementato	
	Non applicabile	

7. Misure di sicurezza specifiche per la fornitura e/o la manutenzione di un sito

7.1 Misure perimetrali applicate al sistema che ospita il sito

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

7.2 SO su cui è poggiato il sito

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

7.3 CMS adottato per lo sviluppo del sito

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

7.4 Plug in

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

7.5 Contratto che preveda di manutenzione sistemistica, aggiornamento CMS e plug in correlati

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

7.6 Software correlati (es. sw di newslettering)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

CARATTERISTICHE DI QUALITÀ, DI SICUREZZA, DI PERFORMANCE E SCALABILITÀ, INTEROPERABILITÀ, PORTABILITÀ DEI SERVIZI CLOUD

8. Qualità aziendale.

Per l'erogazione del servizio cloud, è stato formalmente adottato dal fornitore un sistema di gestione della qualità in conformità allo standard ISO/IEC 9001.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	

	Implementato	
	Non applicabile	

9. Gestione dei servizi IT – Sicurezza dei servizi IT

9.1 Per l'erogazione del servizio, è stato formalmente adottato dal fornitore un sistema di gestione dei servizi IT in conformità allo standard ISO/IEC 20000.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

9.2 Per l'erogazione del servizio, è stato formalmente adottato dal fornitore un sistema di gestione della sicurezza delle informazioni in conformità allo standard ISO/IEC 27001.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

9.3 Per l'erogazione del servizio, solo se in cloud, è stato formalmente adottato dal fornitore un sistema di gestione della sicurezza delle informazioni in linea anche con le linee guida dello standard ISO/IEC 27017 e ISO/IEC 27018.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

10. Attività di supporto

Per il servizio cloud sono garantite attività di supporto ai clienti.
Il servizio di supporto è: (I) fornito esclusivamente in lingua italiana durante le business hours, anche in lingua inglese per le emergenze 24/7; (II) accessibile almeno tramite uno dei seguenti canali preferenziali: recapito telefonico ed e-mail.
In aggiunta, è messo a disposizione dell'Acquirente un sistema di troubleshooting, garantendone anche l'esposizione tramite API per permettere l'interazione programmatica con i casi di supporto.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

11. Censimento apparati fisici

Per l'erogazione del servizio cloud, sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione del fornitore

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

12. Censimento piattaforme e applicazioni software

Per l'erogazione del servizio cloud, sono censite le piattaforme e le applicazioni software in uso nell'organizzazione del fornitore

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	

	Non applicabile	

13. Ruoli e responsabilità inerenti alla cybersecurity

Per l'erogazione del servizio cloud, il fornitore ha definito e reso noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

14. Identificazione delle vulnerabilità

Per l'erogazione del servizio cloud, le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione del fornitore sono identificate e documentate

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

15. Valutazione del rischio

Per l'erogazione del servizio cloud, il fornitore utilizza le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti per determinare il rischio

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

16. Identity Management

Per l'erogazione del servizio cloud, il fornitore amministra, verifica, revoca e sottopone a audit sicurezza le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

17. Controllo degli accessi fisici

Per l'erogazione del servizio cloud, il fornitore protegge e amministra l'accesso fisico alle risorse

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

18. Controllo degli accessi remoti

Per l'erogazione del servizio cloud, il fornitore amministra l'accesso remoto alle risorse

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

19. Privilegio minimo e separazione delle funzioni
Per l'erogazione del servizio cloud, il fornitore amministra gli accessi alle risorse e le autorizzazioni secondo il principio del privilegio minimo e della separazione delle funzioni

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

20. Formazione e addestramento degli utenti
I dipendenti e collaboratori del fornitore hanno ricevuto adeguata formazione sulla protezione dei dati personali e la sicurezza delle informazioni e siete in grado di comprovarlo.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

21. Ruolo e responsabilità degli utenti privilegiati
Gli utenti privilegiati (es. Amministratori di Sistema) del fornitore comprendono i loro ruoli e responsabilità

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

22. Si indicano le persone fisiche che svolgono interventi tipici da Amministratori di Sistema nei sistemi offerti all'acquirente.

	Non ancora implementato o pianificato	Es. Nome Cognome – Backup Manager
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile (non sono forniti servizi IT di alcun tipo)	

23. Localizzazione dei dati
I dati personali, ivi incluse le informazioni relative alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea. Nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di business continuity e di disaster recovery, anche se esternalizzate (ad esempio tramite cloud computing), salvo motivate e documentate ragioni di natura normativa o tecnica.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

24. I dati trattati per conto del Titolare del trattamento, sono trasferiti al di fuori dello Spazio Economico Europeo. SI NO
In particolare verso il seguente Paese Terzo _____
Per tali trasferimenti dei dati extra SEE, è implementato uno degli strumenti di cui agli artt. 44 ss. per assicurare che il livello di protezione delle persone fisiche non sia pregiudicato.

	Non ancora implementato o pianificato	Note/Commenti/Indicare quale strumento è implementato:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

25. Protezione contro l'esfiltrazione dei dati
Per l'erogazione del servizio cloud, il fornitore implementa tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak).

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

26. Integrità dei dati
Per l'erogazione del servizio cloud, il fornitore impiega meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

27. Baseline per la configurazione dei sistemi
Per l'erogazione del servizio cloud, il fornitore definisce e gestisce pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

28. Backup
Per l'erogazione del servizio cloud, il fornitore esegue, amministra e verifica i backup delle informazioni.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

29. Business continuity e Disaster recovery
Per l'erogazione del servizio cloud, il fornitore attiva e amministra piani di risposta (Incident Response e Business Continuity) e recupero (Incident Recovery e Disaster Recovery) in caso di incidente/disastro

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

30. Piano di gestione delle vulnerabilità
Per l'erogazione del servizio cloud, il fornitore ha sviluppato e implementato un piano di gestione delle vulnerabilità

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

31. Manutenzione e riparazione dei sistemi
Per l'erogazione del servizio cloud, il fornitore garantisce che la manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

32. Manutenzione remota

Per l'erogazione del servizio cloud, il fornitore garantisce che la manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

33. Monitoraggio della rete

Per l'erogazione del servizio cloud, il fornitore garantisce lo svolgimento del monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

34. Rilevazione del codice malevolo

Per l'erogazione del servizio cloud, il fornitore garantisce che il codice malevolo viene rilevato

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

35. Monitoraggio del personale, delle connessioni, dei dispositivi e del software

Per l'erogazione del servizio cloud, il fornitore svolge il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

36. Scansione delle vulnerabilità

Per l'erogazione del servizio cloud, il fornitore svolge scansioni per l'identificazione di vulnerabilità

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

37. Mitigazione vulnerabilità

Per l'erogazione del servizio cloud, il fornitore assicura che le nuove vulnerabilità sono mitigate o documentate come rischio accettato

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	

	Non applicabile	

38. Piano di ripristino

Per l'erogazione del servizio cloud, il fornitore assicura che esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

39. Portabilità dei dati, utilizzo di formati open

Il servizio cloud deve garantire la disponibilità di funzionalità e/o API per consentire l'esportazione ed importazione massiva dei dati garantendo l'utilizzo di formati open non proprietari.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

40.Si indicano i Responsabili che intervengono nei trattamenti svolti per conto del Titolare del Trattamento.

	Non ancora implementato o pianificato	Es. Nominativo azienda – Provider Infrastruttura cloud
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile (nessun Responsabile interviene nei trattamenti svolti per conto del Titolare del Trattamento)	

41. Caratteristiche del servizio cloud

Il servizio cloud garantisce le seguenti caratteristiche come da indicazioni NIST SP 800-145 e ISO/IEC 17788:2014:

1) Self-Service provisioning: all'utente deve essere garantito di poter provvedere alla fornitura delle risorse informatiche secondo necessità e in modo automatico, senza ricorrere ad interazione umana. Le richieste di risorse computazionali inerenti al servizio cloud oggetto di qualificazione (o informatiche) devono essere fornite unilateralmente, senza la verifica o l'approvazione del fornitore.
2) Accesso alla rete: per il servizio cloud oggetto di qualificazione devono essere offerte opzioni multiple di connettività alla rete e una di queste deve essere obbligatoriamente basata su rete pubblica (i.e. internet).
3) Pool di risorse: le risorse informatiche relative al servizio oggetto di qualificazione devono essere offerte in un pool, in modo da servire più utenti tramite un modello multi-tenant con risorse virtuali diverse che vengono assegnate e riassegnate in modo dinamico, in base alla domanda degli utenti.
4) Elasticità rapida: deve essere supportato il provisioning e de-provisioning del servizio cloud oggetto di qualificazione.
5) Servizio misurabile: la fornitura a consumo del servizio cloud oggetto di qualificazione deve essere tale che l'utilizzo possa essere monitorato, controllato, segnalato e fatturato;
6) Multi-tenant: le risorse fisiche o virtuali relative al servizio oggetto di qualificazione devono essere allocate in modo tale che più tenant e relative computations e dati siano isolati e inaccessibili l'uno dall'altro.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

42. Meccanismi e modalità di scalabilità del servizio cloud

In merito alla scalabilità del servizio cloud, vengono gestiti e dichiarati i seguenti aspetti:

42.1 il meccanismo di scalabilità offerto (automatico e configurabile, nativo, manuale);

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	

	Implementato	
	Non applicabile	

42.2 la tipologia (orizzontale e/o verticale);

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

42.3 condizione massime di carico sopportabili dal servizio (numero di utenti concorrenti e/o volume di richieste processabili);

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

42.4 le modalità di configurazione (sulla base di metriche di monitoraggio, pianificato nel tempo);

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

42.5 i tempi minimi di reazione del servizio alla richiesta di nuove risorse (i.e. attivazione di nuove risorse).

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

42.6 In aggiunta, il fornitore rende disponibili informazioni trasparenti in merito ad eventuali ulteriori funzionalità accessorie disponibili per il servizio e configurabili dall' Acquirente per gestire la scalabilità ed ottenere parametri migliori.

	Non ancora implementato o pianificato	Note/Commenti:
	Parzialmente implementato o pianificato	
	Implementato	
	Non applicabile	

Con la sottoscrizione del presente questionario, il Responsabile del Trattamento:

b) Si assume la piena responsabilità, civile e penale, della veridicità e dell'accuratezza delle proprie dichiarazioni;

c) Prende atto che, con riferimento ai singoli punti ai quali è stata fornita risposta negativa o parzialmente negativa ("Non ancora implementato o pianificato", "Parzialmente implementato o pianificato"), si configura una totale o parziale violazione della normativa vigente in materia di protezione dei dati personali e s'impegna pertanto a procedere tempestivamente, e comunque prima del conferimento di qualsiasi dato personale da parte del Titolare del Trattamento, alla propria messa in conformità, previo accordo scritto con il Titolare del Trattamento, e conseguente nuova preventiva valutazione, o in alternativa a fornire informazioni integrative, o adeguate motivazioni, alla Scrivente;

d) Prende atto che, anche sulla base dei riscontri al presente questionario e/o di evidenze diverse e ulteriori, il Titolare del Trattamento procede alle necessarie valutazioni ai sensi dell'art. 28 par. 1 e par 3 let. h) del GDPR 2016/679 e si riserva di adottare gli opportuni provvedimenti qualora le non conformità rilevate costituiscano violazione della normativa vigente in materia di protezione dati, incluso il recesso contrattuale per giusta causa.

Verona, __/__/____

Per il Titolare del Trattamento	Per il Responsabile del Trattamento

Per espressa accettazione dei punti a), b), c) e d) della presente.

Per il Responsabile del Trattamento