Allegato A

Misure tecniche ed organizzative per l'esecuzione dei contratti per l'acquisizione di prestazioni, servizi e servizi IT

INDICE DEI CONTENUTI

1. Premesse 3
2. Garanzie del Contraente 3
3. Misure tecniche per la sicurezza dei dati e delle informazioni 5
4. Misure organizzative per la sicurezza dei dati e delle informazioni 9

1. Premesse

Il Committente definisce con le presenti misure tecniche ed organizzative l'insieme dei requisiti che il Contraente si impegna a seguire in relazione all'erogazione di prestazioni, servizi e servizi IT definiti nell'ambito del contratto in vigore tra le Parti.
Il Committente mira a perseguire la sicurezza dei dati e delle informazioni in termini di riservatezza, integrità e disponibilità in coerenza con gli standard e le best practices di Information Security e protezione dei dati personali.

Relativamente all'acquisizione dei servizi IT, è intenzione del Committente consolidare l'evoluzione in ottica cloud computing delle proprie soluzioni IT avviando un'iniziativa di acquisizione di tecnologie e di servizi Cloud.
L'affidamento dei dati in cloud ai sensi della ISO 27017:2015 e della ISO 27018:2019 prevede la verifica di determinati requisiti sia per il Contraente che per il Committente. Il Committente, in completa trasparenza per la gestione dei servizi offerti, fornisce di seguito un riepilogo dei reciproci adempimenti riferiti a quelli che il Committente adotta come "Cliente" (Cloud Service Customer), in ottemperanza alla ISO 27017: 2015 e alla ISO 27018:2019.

In caso di conflitto tra le presenti misure tecniche ed organizzative e qualsiasi termine e condizione stabilito nel Contratto, prevarranno i termini e le condizioni ivi definite unitamente a quelle previste nell'atto di nomina a Responsabile del trattamento ex art. 28 del Regolamento Europeo 2016/679 ("GDPR"), ove applicabile.
In caso di discordanza tra quanto previsto nel presente atto e quanto contenuto nell'anzidetto atto di nomina a Responsabile del trattamento ex art. 28 del Regolamento Europeo 2016/679 ("GDPR"), prevarranno le previsioni contenute nell'atto di nomina.

Nel caso di acquisizione di servizi IT le clausole di seguito previste sono parte integrante delle condizioni generali di fornitura e definiscono le caratteristiche e i requisiti richiesti dal Committente. Le condizioni, le appendici e i documenti ivi richiamati, ancorché non materialmente allegati, costituiscono parte integrante e sostanziale del Contratto.

2. Garanzie del Contraente

Il Contraente adotta una serie di misure, controlli e prassi operative volte a garantire la sicurezza delle informazioni e la protezione dei dati personali, quando presenti.

Nel caso in cui nella fornitura di prestazioni e servizi, il Contraente venisse a conoscenza di dati personali, nonché effettuasse trattamento degli stessi, il Contraente espressamente riconosce e garantisce che tratterà tali dati in conformità alle disposizioni della Legge in materia di protezione dei dati personali e, nel caso in cui il Contraente sia nominato Responsabile del trattamento, ex art. 28 del Reg. EU 2016/679 ("GDPR"), secondo le modalità e i termini previsti nell'atto di nomina stesso.

Nel caso di servizi relativi a dati personali comuni e/o dati classificati dal Committente almeno come "internal"[1], il Contraente garantisce, almeno per la fornitura di servizi IT, l'applicazione di metodi e processi certificati da terzi in ambito ISO/IEC 27001:2013 e, in aggiunta, nel caso di servizi inerenti il Cloud computing, ISO/IEC 27017:2015 e ISO/IEC 27018:2019 e ISO27701:2019. Nel caso di indisponibilità delle presenti certificazioni, previo accordo con il Committente, il Contraente deve dimostrare di adottare e/o implementare

[1] Informazioni la cui eventuale divulgazione o diffusione non autorizzata all'esterno potrebbe essere inappropriata e/o creare danni o problematiche alla Società

misure di sicurezza affini, conformi e coerenti con i suddetti standard internazionali e successive modificazioni per l'intera durata del/i Contratto/i.
In entrambi i casi il Contraente dovrà comunque garantire, come indicato al precedente capoverso, l'adozione di misure di sicurezza ai sensi dell'art.32 GDPR.

In alternativa alle succitate certificazioni, il Committente potrà valutare l'adeguatezza delle misure, dei controlli e delle prassi operative volte a garantire la sicurezza delle informazioni attuate dal Contraente sulla base di ulteriori certificati o report (es. ISAE 3402, SOC 2, SOC 3, CSA Star, etc.) che il Contraente stesso metterà a disposizione in visualizzazione al Committente.

Sempre in caso di fornitura di servizi IT, il Contraente garantisce per il servizio SaaS: (i) di avere il diritto di concedere in licenza il software che costituisce il Servizio; (ii) che detto software funzionerà secondo quanto descritto nella Documentazione tecnica condivisa; (iii) che il Servizio sarà fornito con adeguata perizia, diligenza e professionalità in linea con l'attuale prassi commerciale del settore; e (iv) che il Servizio sarà erogato nel rispetto degli SLA descritti nel contratto di fornitura.
Il Contraente garantisce di avere il diritto di concedere le licenze d'uso messe a disposizione per gli utenti per i software forniti dal Contraente o software di Terzi in conformità ai diritti d'autore.
Le garanzie non coprono eventuali carenze o danni dovuti a: (i) interazione con Applicazioni di Terzi e/o con software, servizi o contenuti non del Contraente; (ii) qualsiasi connettività fornita da terzi; (iii) qualsiasi funzionamento difforme da quanto indicato nella Documentazione che sia causato dall'uso del Servizio in modo non conforme con le condizioni d'uso dei servizi cloud.

Il Contraente garantisce la possibilità al Committente di richiedere Audit di seconda parte, mediante un preavviso da inviare tramite pec entro 5 giorni dalla data di esecuzione della verifica, oltre a quanto già previsto nell'eventuale atto di nomina a Responsabile del trattamento ex art. 28 GDPR. Dove non ci sia la possibilità di eseguire audit da parte del Committente, il Contraente mette a disposizione la visione dei certificati ottenuti in conformità agli standard UNI ISO 27001:2017 e sue estensioni e/o di altre ulteriori certificazioni in suo possesso (es. SOC, etc.).

Il Contraente effettua periodiche rivalutazioni dell'analisi dei rischi per confermare l'adeguatezza delle misure di sicurezza attuate in relazione alla fornitura di prestazioni e servizi definita nell'ambito del Contratto.

Il Contraente non potrà comunicare né diffondere i dati personali oltre ai casi previsti nel Contratto e nell'eventuale atto di nomina a Responsabile ex art. 28 GDPR, senza aver ottenuto apposita autorizzazione da parte del Committente con le eventuali istruzioni scritte, salvo che la comunicazione degli stessi non sia prescritta da una disposizione normativa o regolamentare imperativa; in tale circostanza è onere del Contraente informare il Committente.
Il Contraente si impegna a limitare al massimo l'utilizzo di materiale cartaceo contenente dati personali del Committente.
Qualora il Contraente sia un provider del servizio IT richiesto, esso si impegna a collocare i dati della Committente sempre e solo su server all'interno dell'Unione Europea. In tal caso il Contraente, nell'ambito dei servizi cloud, offre al Committente la garanzia di poter:

- cambiare il proprio Cloud Service Provider;
- riportare al proprio interno il servizio se gestito da un Cloud Service Provider esterno;
- affidare a un Cloud Service Provider esterno un servizio gestito internamente nel proprio cloud privato.

Il Contrante si impegna a favorire l'eventuale migrazione delle informazioni della Committente e verranno stabilite tra le Parti, con un separato atto, specifiche istruzioni vincolanti che specificheranno in modo completo ed esaustivo tutte le condizioni e le modalità operative di uscita dal servizio (c.d. Transfer-Back), con particolare riferimento a:

- le modalità con le quali vengono forniti i dati e, se del caso, il codice applicativo;

- le modalità di erogazione del supporto alla migrazione;
- i tempi, gli effort previsti e gli eventuali step transitori.

2.1. Manutenzione, monitoraggio e supporto

Il Contraente monitora regolarmente la fornitura di prestazioni e servizi con personale dedicato ed eventuali strumenti automatici.
Il Contraente mette a disposizione del Committente i servizi di assistenza e applica aggiornamenti periodici al servizio per migliorarne la sicurezza e/o le prestazioni. Gli aggiornamenti al servizio non includono la messa a disposizione di nuove componenti di servizio.

Relativamente ai servizi IT il Contraente, oltre ai servizi standard di assistenza, applica aggiornamenti periodici al servizio per migliorarne, oltre la sicurezza e/o le prestazioni, la funzionalità. Alcuni aggiornamenti potrebbero rimuovere o ridurre funzionalità, comunque in misura non sostanziale.
Per le attività di manutenzione programmata, il Contraente può cambiare la finestra di Manutenzione Programmata di routine, spostandola ad una finestra alternativa di pari durata, dandone al Committente comunicazione per posta elettronica con un preavviso di 7 giorni.
Per le attività di manutenzione di emergenza, il Contraente ne darà comunicazione al Committente in tempi brevi e comunque il prima possibile. Il Contraente adotterà tutte le misure necessarie per ridurre al minimo l'impatto sul servizio erogato al cliente durante le attività di manutenzioni d'emergenza.

2.2. Ubicazione, inventario e etichettatura degli asset informatici e non

Relativamente agli asset informatici il Contraente in qualità di provider del servizio colloca i dati del Committente sempre e solo su server all'interno dell'Unione Europea.
Il Contraente gestirà, identificherà ed etichetterà i dati forniti dal Committente in relazione alla diversa tipologia di informazioni e dandone evidenza a richiesta.

Con riferimento agli asset non informatici (esempio archivi cartacei con dati personali) il Contraente garantisce:

- la custodia di tali asset in zone di lavoro ad accesso controllato e limitato alle sole persone autorizzate;
- la catalogazione degli asset cartacei;
- ove richiesto, la distruzione, esauriti i tempi di retention previsti, della documentazione cartacea in modo che i dati personali ivi contenuti non siano più consultabili ed intellegibili.

2.3. Dismissione sicura o riutilizzo delle apparecchiature IT

Il Contraente ha il compito di dismettere in modo sicuro le apparecchiature (anche ai fini del riutilizzo) secondo i principi della ISO 27001.

3. Misure tecniche per la sicurezza dei dati e delle informazioni

3.1. Protezione da malware

I sistemi del Contraente sono protetti contro i malware mediante l'utilizzo di antivirus mantenuti costantemente aggiornati. In particolare, sono adottate adeguate misure di sicurezze per prevenire, rilevare ed eliminare virus informatici o altri programmi dannosi. Il Contraente mantiene costantemente aggiornati i sistemi operativi, gli antivirus, i firewall ed altri programmi per la sicurezza delle informazioni e dei dati personali.

3.2. Credenziali di autenticazione

I sistemi sono configurati con modalità atte a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione univoche (username e password), non riassegnabili agli utenti neppure in tempi diversi.
Nell'ambito dell'erogazione dei servizi cloud, il Contraente garantisce la registrazione/de-registrazione degli utenti interni al Committente ai vari servizi in cloud.

3.3. Password

La parola chiave (i.e. password) presenta, al minimo, le seguenti caratteristiche di sicurezza di base: obbligo di modifica al primo accesso, lunghezza minima, regole di complessità, scadenza, history, valutazione contestuale della robustezza e archiviazione dell'hash.
Deve essere imposto un formato della password per evitare l'utilizzo di password banali o che contengano riferimenti agevolmente riconducibili all'utente al fine di garantire che le password siano adeguatamente robuste. Inoltre, il Contraente assicura che le password non siano salvate né trasmesse in chiaro.
Il Contraente si assicura che tutti gli utenti siano sensibilizzati circa le modalità di conservazione sicura delle password, come ad esempio: evitare di comunicare a terzi la propria parola chiave, modificare la password in caso di compromissione, etc..
Il Contraente che eroga servizi Cloud garantisce l'osservanza di procedure definite per la gestione delle password del Committente.

3.4. Log management

I sistemi sono configurati con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze, incluse quelle degli Amministratori di Sistema, e protetti da adeguate misure di sicurezza che ne garantiscono l'integrità, la riservatezza e la disponibilità.
Il Contraente implementa un set di log standard che consentono di monitorare una serie di eventi e rilevare eventuali attacchi. Ciò non toglie che il Committente è tenuto a verificare se tale set di log è sufficiente e in linea con le proprie politiche; diversamente, deve definire con il Contraente i requisiti per la registrazione degli eventi e verificare che il servizio soddisfi tali requisiti.
I log sono analizzati con adeguata frequenza e con strumenti automatici (es. sistema centralizzato di Security Information and Event Management) al fine di verificare che non ci siano state anomalie.
Il Contraente che eroga servizi Cloud garantisce l'adozione di un sistema centralizzato di event logging e dà la possibilità al Committente di esportare i log sui propri sistemi.

3.5. Continuità operativa

Il Contraente adottata idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi in tempi certi (es. procedure di backup, prove di ripristino dei dati, etc.).

Sono predisposti dal Contraente un piano di continuità operativa e di disaster recovery che comprendono le attività per rispondere, recuperare, riprendere e ripristinare a un livello predefinito i servizi a seguito di un'interruzione degli stessi anche nel caso di eventi avversi di portata rilevante, applicando le buone pratiche presenti nello standard ISO/IEC 22313.

Il Committente può richiedere le specifiche sulle modalità di esecuzione del backup (RPO, retentions, ecc.) e, laddove previsto da contratto, la condivisione dei piani di BC e DR.

3.6. Vulnerability Assessment & Penetration Test

Il Contraente adotta misure utili a identificare immediatamente le vulnerabilità non appena diventano note e procede con gli opportuni aggiornamenti per risolvere le vulnerabilità.
Il Contraente effettua periodicamente attività di analisi delle vulnerabilità tecniche, sia in relazione agli ambiti infrastrutturali sia a quelli applicativi. Ove ritenuto appropriato in relazione ai potenziali rischi identificati, tali verifiche sono integrate periodicamente con Penetration Test, mediante simulazioni di intrusione che utilizzano diversi scenari di attacco. I risultati delle verifiche sono puntualmente e dettagliatamente esaminati per identificare e attuare le migliorie necessarie a garantire il livello di sicurezza atteso.
Il Contraente si impegna ad installare le patch di sicurezza disponibili per i componenti del sistema e i programmi software in uso; devono essere eseguiti appropriati test prima della loro distribuzione.
Il Contraente che eroga servizi Cloud, in caso di servizio SaaS, dichiara se le componenti che costituiscono il servizio sono state sottoposte ai test OWASP con esito positivo.

3.7. Amministratori di Sistema

Relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il monitoraggio. Tale elenco dovrà poter essere condiviso con il Committente su richiesta.

3.8. Gestione degli incidenti

Il Contraente assicura una risposta rapida ed efficace agli incidenti relativi alla sicurezza delle informazioni attraverso l'implementazione di sistemi e l'esecuzione di attività in linea quanto definito all'interno delle Condizioni Generali di Acquisto e coerenti con quanto raccomandato dagli standard di sicurezza internazionali (p.e. ISO/IEC 27002, ISO/IEC 27035), e garantisce la notifica degli stessi al Committente nel rispetto di quanto previsto nell'atto di nomina ex art. 28 GDPR e all'art. 33 GDPR. Il Contraente assicura la massima trasparenza nella gestione degli eventi di sicurezza, garantendo al Committente appropriata visibilità dei processi di issue tracking e assistenza tecnica.
Il Contraente deve definire le tempistiche per la presa in carico e gestione degli eventi di sicurezza in funzione di diverse priorità, dichiarando i livelli di servizio garantiti.

3.9. Gestione dei supporti rimovibili

Il Contraente definisce le modalità di gestione sicura dei supporti rimovibili (dispositivi portatili, dischetti, CD, DVD ecc.), per proteggere i supporti e formattarli.
I supporti rimovibili sono protetti dalle sole operazioni di scrittura o dalle operazioni di lettura e scrittura, inoltre deve essere impedito il trasferimento di dati su media non consentiti.
Le periferiche non più utilizzate, devono essere disabilitate onde evitare l'accesso da parte di utenti non autorizzati e l'inserimento di software maligno.
I supporti rimovibili se non utilizzati sono distrutti o resi inutilizzabili, altrimenti possono essere riutilizzati se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

3.10. Sicurezza Fisica

L'accesso fisico ai locali e ai Data Center del Contraente deve essere regolato da procedure interne e limitato ai soli soggetti autorizzati.
Il Contraente si impegna ad assegnare servizi di Data Center a subfornitori, nominati sub-responsabili, che garantiscano appropriate e idonee misure di sicurezza per assicurare, nel tempo, la riservatezza, la disponibilità e l'integrità dei dati personali ivi conservati e trattati, ai sensi dell'art. 32 GDPR.
In tale caso l'accesso ai locali ed ai Data Center dovrà essere regolato nel rispetto di quanto indicato al primo capoverso del presente 3.10.

Il Contraente che eroga servizi Cloud rende nota la localizzazione dei data center propri e/o dell'infrastruttura Cloud utilizzata per erogare anche parzialmente il servizio e/o all'interno dei quali transiteranno anche temporaneamente i dati gestiti dal servizio (ivi compresi i siti di disaster recovery e di backup).

3.11. Sicurezza delle comunicazioni

Sono adottati dal Contraente protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile. Il Contraente, inoltre, prevede l'utilizzo di canali di comunicazione cifrati e sicuri per lo scambio di informazioni verso l'esterno e l'interno, adeguati alla criticità delle informazioni trattate.

In particolare, i flussi dati da e verso i sistemi in cloud esposti su internet sono protetti utilizzando un canale sicuro TLS in modo da assicurare:
- Autenticazione del server (chiave RSA da 2048 bit)
- Cifratura della sessione con algoritmo di cifratura simmetrico, considerato ragionevolmente sicuro alla data, con una chiave di sessione di almeno 128 bit.

3.12. Crittografia

Il Contraente implementa misure tecniche di crittografia sui propri sistemi adottando meccanismi di cifratura con un livello di robustezza adeguato rispetto alla criticità delle informazioni trattate.
Il Contraente che eroga servizi Cloud dichiara quale tipo di crittografia utilizza per proteggere la riservatezza dei dati scambiati con il Committente e per proteggere la riservatezza dei dati archiviati presso i Data Center.

3.13. Network

Il Contraente adotta misure di sicurezza adeguate a prevenire e mitigare qualsiasi evento di sicurezza che potrebbe comprometterne le funzionalità delle componenti di rete tra cui, ad esempio, attraverso l'utilizzo di firewall, sonde IPS (i.e. Intrusion Prevention System), strumenti di analisi del traffico, etc. I sistemi di rilevamento intrusione sono mantenuti aggiornati in relazione alle migliori tecnologie disponibili.
Il Contraente assicura la segregazione delle reti da quelle utilizzate dal Committente.
Il Contraente che eroga servizi Cloud assicura l'osservanza di una Policy di sicurezza delle informazioni per la configurazione delle reti virtuali VLAN.

3.14. Change Management

Il Committente implementa un processo di change management, al fine di garantire che vengano utilizzate procedure e metodi standard per la gestione tempestiva ed efficiente di ogni cambiamento nell'ambito dell'infrastruttura e dei servizi offerti.
Il Contraente che eroga servizi Cloud garantisce l'applicazione di misure di sicurezza per separare logicamente l'ambiente virtuale del Committente da quello degli altri Clienti e impedire di accedere o esporre il contenuto

a persone non autorizzate. Inoltre, il Contraente garantisce la disponibilità tempestiva di informazioni al Committente circa i cambiamenti e le migliorie introdotte in seguito ad aggiornamenti apportati alle modalità di funzionamento e fruizione dei servizi erogati. È definito un periodo temporale prima del quale il Committente deve dare comunicazione al Committente degli interventi di manutenzione attraverso un canale di comunicazione diretto.

3.15. Hardening

Il contraente pone in essere apposite attività di hardening finalizzate a prevenire il verificarsi di eventi avversi minimizzando le debolezze architetturali dei sistemi operativi, delle applicazioni e degli apparati di rete.
Qualora non fossero presenti le procedure, è necessaria la predisposizione del software di base in modalità sicura attraverso, a titolo esemplificativo e non esaustivo, l'eliminazione dei servizi non necessari, l'eliminazione delle utenze non necessarie, la modifica delle password di default, etc.

3.16. Sincronizzazione degli orologi

Tutti i sistemi cloud del Contraente utilizzano il protocollo sicuro per la sincronizzazione degli orologi. Il fuso orario utilizzato è CEST.

4. Misure organizzative per la sicurezza dei dati e delle informazioni

4.1. Ruoli e responsabilità

Il Contraente:

- definisce, formalizza le responsabilità e i doveri di ciascuna figura 'interna' alla Società stessa (Contraente) coinvolta nell'ambito dei processi di governo e gestione dei dati personali delle persone fisiche, ivi compreso il rispetto dei compiti e delle funzioni svolte dal DPO previsti dall'art. 39 del GDPR;
- attua, qualora necessario, la nomina formale di un altro sub-Responsabile del Trattamento;
- identifica e incarica formalmente una figura interna (il Data Protection Officer o il Titolare stesso del Contraente) per lo svolgimento dei compiti di cooperazione con l'Autorità Garante per la protezione dei dati personali e comunica alla stessa il nominativo e i dati di contatto della figura individuata.

Il Contraente, inoltre, identifica e comunica al Committente un referente per la sicurezza delle informazioni responsabile del coordinamento e del monitoraggio delle norme e procedure sulla sicurezza.

4.2. Policy, istruzioni per gli incaricati e Disciplinari utenti

Il Contraente documenta i criteri e i principi normativi che sono adottati in qualità di Responsabile del trattamento per garantire la protezione dei dati personali e per evitare la comunicazione e/o diffusione di tali dati al di fuori dei casi previsti e consentiti dalla normativa privacy. Il Contraente inoltre garantisce la predisposizione e la comunicazione a ciascun incaricato delle istruzioni operative.

Relativamente ai servizi IT il Contraente applica regolamenti che tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di rispettare e che sono finalizzati a garantire comportamenti idonei ad assicurare la protezione dei dati nell'utilizzo delle risorse informatiche.

4.3. Autorizzazione accessi

Il Contraente garantisce che nell'espletamento delle mansioni e dei compiti conferiti, l'incaricato adotta comportamenti di massima riservatezza in ordine ai dati personali ed alle informazioni oggetto di trattamento, impegnandosi a non divulgare, neanche dopo il venir meno dell'autorizzazione al trattamento, alcuna delle informazioni di cui è venuto a conoscenza.

L'autorizzazione decade per revoca o per il venir meno dei compiti e delle mansioni che legittimano il trattamento dati stesso.

Per gli accessi logici il Contraente definisce una procedura per la gestione del ciclo di vita delle utenze che comprende, tra le altre, le fasi di creazione, disabilitazione temporanea, disabilitazione definitiva, modifica del profilo di autorizzazione dell'utenza e revisione periodica.
I profili di autorizzazione sono definiti in funzione delle mansioni assegnate in modo da consentire l'accesso ai soli dati necessari per effettuare le operazioni relative ai trattamenti di competenza. Tali profili sono oggetto di controlli periodici.

4.4. Gestione dei trattamenti dei dati personali

Il Contraente documenta i criteri, i principi e le modalità di gestione della protezione dei dati personali degli interessati in ottemperanza alle previsioni del GDPR..

Il Contraente predispone e mantiene aggiornato il registro dei trattamenti con riguardo a tutte le informazioni riportate nell'art. 30 del GDPR.

Il Contraente disciplina i trattamenti svolti da parte di un Responsabile del trattamento (nominato ex art. 28, co.4, GDPR) in un contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.

Il Contraente definisce le linee guida e le regole che le strutture aziendali devono seguire qualora si verifichi un incidente di sicurezza che comporta una violazione di dati personali nell'ambito delle attività di trattamento svolte ("data breach"), con impatto sui diritti e le libertà dei soggetti interessati.

4.5. Gestione interventi di assistenza IT

Gli interventi di assistenza garantiscono l'esecuzione delle sole attività previste contrattualmente per impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Committente.
Il Contraente fornisce, laddove previsto, la documentazione tecnica, le guide d'uso e/o altro materiale di supporto, ivi compresa la documentazione dettagliata delle API e delle interfacce CLI, GUI e SOAP/REST, se previste dal servizio.
Il Contraente che eroga servizi Cloud fornisce al Committente un servizio di supporto tecnico con costi e orari di servizio definiti.
Il supporto deve essere accessibile mediante opportuni canali di comunicazione e adeguati sistemi di gestione (issue tracking), al fine di consentire al Committente di effettuare in completa autonomia le segnalazioni di malfunzionamenti e potenziali pericoli per la sicurezza e la fruibilità del servizio.
Il Contraente che eroga servizi Cloud dichiara gli obiettivi corrispondenti agli indicatori di qualità del servizio sotto riportati e ne garantisce il rispetto nei rapporti contrattuali:

- Availability (Percentuale di tempo in cui il servizio risulta essere accessibile e usabile)
- Support hours (L'orario in cui il servizio di supporto tecnico è operativo)

- Maximum First Support Response Time (Il tempo massimo che intercorre tra la segnalazione di un inconveniente da parte del cliente e la risposta iniziale alla segnalazione)
- Cloud Service Bandwidth (La quantità di dati che può essere trasferita in un determinato periodo di tempo.)
- Limit of Simultaneous Connections (Numero massimo di connessioni simultanee supportate dal servizio.)
- Cloud Service Throughput (Numero di transazioni processate in ciascuna unità di tempo dal servizio.)
- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Backup Interval (tempo che intercorre tra un backup e l'altro.)
- Retention period of backup data
- Data retention period (Il periodo di tempo in cui i dati del cliente vengono mantenuti dal CSP dopo la notifica di cessazione del servizio.)
- Log retention period (l periodo di tempo in cui i file di log relativi al servizio vengono conservati dopo la notifica di cessazione del servizio.)

4.6. Change Management

Il Contraente applica una specifica procedura di gestione dei cambiamenti in considerazione dell'introduzione di eventuali innovazioni tecnologiche o cambiamenti della propria impostazione e della propria struttura organizzativa.
Il Contraente integra i processi di Project Development e Change Management con i principi di privacy by design/by default. In particolare, sin dalla fase di progettazione di una nuova iniziativa e per l'intero ciclo di vita dei dati personali coinvolti:
- definisce chiari obiettivi di protezione quali la riservatezza, l'integrità e la disponibilità dei dati personali;
- prevede (implementa e testa) misure tecnico-organizzative di sicurezza volte ad attuare in modo efficace i principi di protezione dei dati personali, tutela i diritti degli interessati, e garantisce che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità di trattamento (principio di minimizzazione).

4.7. Sviluppo sicuro e test per servizi IT

L'ambiente di sviluppo software del Contraente è accessibile esclusivamente al personale a ciò preposto. Il processo di sviluppo del Contraente segue rigide linee guida di sviluppo sicuro finalizzate a garantire il rispetto dei principi di Security by Design. I test del codice segue un processo predefinito finalizzato a valutare sia la funzionalità del codice sia la presenza di vulnerabilità gravi. Il passaggio in produzione avviene in modo automatico, ma le modifiche vengono opportunamente tracciate. Gli ambienti di sviluppo, test e produzione sono fisicamente e logicamente separati.

4.8. Formazione

Il Contraente eroga periodicamente ai propri dipendenti coinvolti nelle attività gestione dei servizi corsi sulla sicurezza delle informazioni e sulla corretta gestione dei dati personali nonché sulle proprie politiche e procedure pertinenti il servizio erogato.

4.9. Audit interni

Il Contraente assegna a personale esterno qualificato l'esecuzione di audit interni sulla sicurezza delle informazioni e sulla privacy; la periodicità di tali attività è specificata nel programma almeno annuale degli audit.