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

INDICE DEI CONTENUTI

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.

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 nell'ambito della fornitura di prestazioni e servizi, il Contraente venisse a conoscenza di dati personali, di cui la Committente è Titolare, 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 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 successive modificazioni, 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 misure di sicurezza affini, conformi e coerenti con i suddetti standard internazionali e successive modificazioni e in ogni caso in linea con i requisiti richiesti dal presente documento 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

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

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, o di sanitizzarle ai fini del riutilizzo, secondo i principi della ISO 27001. Ulteriori best practices sono riportate nel documento NIST SP 800-88r1.

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

La tabella che segue indica le misure di sicurezza tecniche e organizzative che devono essere garantite dal Contraente per l'esecuzione dei contratti per l'acquisizione di prestazioni e servizi IT e, nell'ambito degli stessi, per l'espletamento dell'eventuale trattamento dei dati personali. I servizi e le prestazioni IT di cui ASPI si avvale per mezzo di Fornitori esterni sono stati raggruppati per tipologia individuando i seguenti cluster:

- **Professional Services** - Servizi di progettazione e design di nuovi processi e servizi, servizi di advisoring;
- **Application Development Services** - Servizi di sviluppo software per soluzioni tecnologiche e gestionali, servizi di customizzazione di software, software retail subscriptions procurement;
- **Application Management Services** - Servizi di manutenzione applicativa, gestione operativa delle applicazioni, servizi VAPT, servizi di system integration, aggiornamento software/firmware

dispositivi IoT;

- **Cloud Services** - SaaS, PaaS, IaaS (Servizi cloud, Licenze cloud, manutenzione e sviluppo dell'infrastruttura cloud, assistenza tecnica);
- **Infrastructure & System Maintenance** - Servizi di manutenzione infrastrutturale e sistemistica (e.g. servizi sistemistici, servizi di assistenza e manutenzione, installazione e configurazione hardware, anche dispositivi IoT, utenze telefoniche e internet);
- **Hardware Procurement** - Servizi di approvvigionamento di componenti fisiche e materiali di qualsiasi apparecchiatura elettronica (router, switch, firewall, server, laptop, mobile device).

In caso di forniture di software retail subscriptions procurement (cfr. cluster Application Development Services) in cui il Contraente si configura esclusivamente come un reseller di licenze di un software di proprietà di terze parti (non effettua dunque alcun servizio di customizzazione, configurazione, sviluppo del software), le misure di sicurezza che dovranno essere garantite dal Contraente non sono quelle applicabili all'intero cluster ADS ma saranno valutate di volta in volta dal Committente sulla base della specifica fornitura.
Di seguito si riporta la tabella riepilogativa dei requisiti di sicurezza tecnici e organizzativi che il Contraente si impegna a sottoscrivere laddove applicabile al servizio IT fornito e nell'ambito di questo, ove presente, al trattamento di dati personali.

La tabella riporta in colonna i cluster di servizi IT sopra elencati, indicando con una "X" in corrispondenza di ciascun requisito (riportato in riga) quelli applicabili al cluster specifico. Si noti che una prestazione o servizio IT può ricadere contestualmente in più cluster, in tal caso il Contraente si impegna a garantire i requisiti di sicurezza applicabili a tutti i cluster che contengono il servizio erogato.
Ad esempio, un contratto che include un servizio di consulenza di progettazione e sviluppo e la conseguente attività di sviluppo software ricade sia nel cluster "Consulenza strategica" sia nel cluster "Application Development Services", pertanto il Contraente si impegnerà a garantire tutti i requisiti applicabili all'uno e all'altro cluster singolarmente.
La colonna denominata "Applicabile ai Sistemi ASPI" riporta "Si" in corrispondenza di tutti i requisiti che solo il Contraente che opera sui sistemi di proprietà di ASPI si impegna a rispettare.
Se invece tale campo non risulta non popolato, il requisito corrispondente deve essere garantito dal Contraente sui propri sistemi, per garantire la protezione delle informazioni di ASPI trattate nell'ambito dei servizi IT erogati.

In coerenza con quanto sopra riportato e in merito al servizio IT oggetto di Fornitura sono da ritenersi applicabili tutte le misure di sicurezza tecniche e organizzative riportate nella seguente tabella per la/e categoria/e:

- **Professional Services**
- **Application Development Services**
- **Application Management Services**
- **Cloud Services**
- **Infrastructure & System Maintenance**

- **Hardware Procurement**
- **Reseller di licenze di un software di proprietà di terze parti**

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Protezione da malware	**1**	I sistemi del Contraente devono essere protetti contro i malware mediante l'utilizzo di idonei strumenti di protezione come, ad esempio, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), antivirus e anti-malware mantenuti costantemente aggiornati. In particolare, sono adottate adeguate misure di sicurezza 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.	X	X	X	X	X		
TECH	Credenziali di autenticazione	**2**	Il Contraente che accede ai sistemi del Committente si impegna a comunicare tempestivamente al Committente i casi di trasferimento e cessazione dell'operatività del personale coinvolto nell'erogazione del servizio, al fine di consentire al Committente una corretta gestione delle utenze e dei relativi privilegi di accesso.	X	X	X	X	X		SI
TECH	Credenziali di autenticazione	**3**	I sistemi del Contraente devono essere configurati con modalità atte a consentire l'accesso unicamente a soggetti dotati di credenziali di autenticazione univoche (username e password), non riassegnabili agli utenti neppure in tempi diversi al fine di evitare che accessi indebiti ai sistemi del Contraente diano accesso ai dati del Committente.	X	X	X	X	X		
TECH	Credenziali di autenticazione (Cloud)	**4**	Nell'ambito dell'erogazione dei servizi cloud, il Contraente deve garantire la registrazione/de-registrazione degli utenti interni al Committente ai vari servizi in cloud.				X			
TECH	Password	**5**	Le password utilizzate dal Contraente sui propri sistemi devono presentare, 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..	X	X	X	X	X		

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Password	**6**	Il Contraente deve assicurare che le password utilizzate per accedere ai sistemi del Committente non siano salvate né trasmesse in chiaro. Il Contraente, inoltre, assicura che tutti gli utenti siano sensibilizzati circa le modalità di conservazione sicura delle password.	X	X	X	X	X		SI
TECH	Password (Cloud)	**7**	Il Contraente che eroga servizi Cloud deve garantire l'accesso in Single Sign On (SSO). In alternativa il Contraente deve garantire l'osservanza di procedure definite per la gestione delle password del Committente.				X			
TECH	Log Management	**8**	I sistemi del Contraente 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. 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.	X	X	X	X	X		
TECH	Log Management	**9**	Le applicazioni (da installare on-premise) che il Contraente fornisce al Committente 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. Inoltre, il Committente può 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. Il Contraente dà la possibilità al Committente di esportare i log sui propri sistemi, secondo quanto richiesto dalle soluzioni tecnologiche adottate dal committente.		X	X		X		SI

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Log Management (Cloud)	**10**	Il Contraente che eroga servizi Cloud garantisce che i sistemi e/o applicazioni 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. Il Committente ritiene sufficiente il seguente set di log: - Autenticazione - Autorizzazione - Gestione della configurazione - Attività degli amministratori - Gestione degli accessi - Attività svolte sui dati con particolare attenzione ai dati personali - Utilizzo di funzionalità a più alto rischio - Connessioni di rete Inoltre, il Committente può 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. 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, secondo quanto richiesto dalle soluzioni tecnologiche adottate dal committente.				X			
TECH	Continuità Operativa	**11**	Il Contraente adotta idonee misure per garantire il ripristino dell'accesso ai dati del Committente in tempi certi in caso di danneggiamento degli stessi (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.	X	X	X	X	X		
TE	Continuità Operativa	**12**	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.		X	X	X	X		

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	VA/PT	**13**	Il Contraente che sviluppa software o effettua manutenzione delle applicazioni per il Committente adotta misure utili a identificare le vulnerabilità non appena diventano note e procede a comunicarle al Committente avviando lo sviluppo di opportuni aggiornamenti per risolvere tali vulnerabilità. Il Contraente, in coerenza con le best practice nazionali (es. AGID) e internazionali (es. NIST) per lo sviluppo di software sicuro e nel rispetto dei principi di "Security by Design" effettua in accordo con il Committente lo svolgimento di attività di Code Review e Penetration Test (PT) sui sistemi del Committente utilizzati per fornire il servizio al fine di prevenire l'introduzione di vulnerabilità.		X	X		X		SI
TECH	VA/PT	**14**	Il Contraente adotta sui propri sistemi e applicazioni 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.	X	X	X	X	X		
TECH	VA (IoT)	**15**	Il Contraente che produce dispositivi IoT o effettua manutenzione di dispositivi IoT per il Committente adotta misure utili a identificare le vulnerabilità non appena diventano note e procede a comunicarle al Committente avviando lo sviluppo di opportuni aggiornamenti per risolvere tali vulnerabilità.		X	X		X		SI
TECH	Test di Sicurezza (IoT)	**16**	Il Contraente che sviluppa software per dispositivi IoT dichiara se le componenti che costituiscono il servizio sono state sottoposte con esito positivo ai test descritti nei documenti OWASP "Application Security Verification Standard) (ASVS) e Mobile Application Security Verification Standard (MASVS)".			X				
TECH	Test di Sicurezza (Cloud)	**17**	Il Contraente che eroga servizi Cloud, in caso di servizio SaaS, dichiara se le componenti che costituiscono il servizio sono state sottoposte con esito positivo ai test descritti nel documento OWASP "Web Security Testing Guide (WSTG)".				X			

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Amministratori di Sistema	**18**	Il Contraente implementa policy e procedure interne per garantire, mediante validi documenti identificativi, la corretta identificazione e profilazione degli utenti inclusi quelli privilegiati (es. amministratori di sistema, utenti di emergenza, utenze tecniche), distinguendo fra utenti interni ed esterni, laddove applicabile, che accedono alle componenti di sistema che gestiscono i dati del Committente.	X	X	X	X	X		
TECH	Amministratori di Sistema	**19**	Il Contraente, al quale sono stati assegnate una o più utenze con privilegi amministrativi per accede ai sistemi del Committente, si impegna a mantenere e aggiornare la lista delle utenze attive e a richiedere al Committente le sole abilitazioni necessarie a svolgere le mansioni che gli sono assegnate in coerenza con i principi del need to know e least privilege.	X	X	X	X	X		SI
TECH	Gestione degli incidenti	**20**	Il Contraente definisce le regole che le proprie strutture aziendali devono seguire per assicurare una risposta rapida ed efficace a fronte del verificarsi di un incidente relativo alla sicurezza delle informazioni; tali regole devono prevedere l'implementazione di sistemi e l'esecuzione di attività in linea con 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 27701, ISO/IEC 27035), e garantire la notifica degli stessi al Committente nel rispetto di quanto previsto nell'atto di nomina ex art. 28 GDPR e all'art. 33 GDPR laddove siano coinvolti dati personali del Committente. 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.	X	X	X	X	X		
TECH	Gestione dei supporti rimovibili	**21**	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 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.	X	X	X	X	X		

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Sicurezza Fisica	**22**	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 che assegna servizi di Data Center a sub-fornitori nominati sub-responsabili deve garantire che questi ultimi implementino 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. Anche in tale caso l'accesso ai data center dovrà essere regolato da procedure interne e limitato ai soli soggetti autorizzati.	X	X	X	X	X		
TECH	Sicurezza Fisica	**23**	Il Contraente che eroga servizi ICT nell'ambito dei quali tratta dati riservati del Committente, rende nota la localizzazione dei propri data center e degli end-point all'interno dei quali transiteranno anche temporaneamente i dati gestiti dal servizio (ivi compresi i siti di disaster recovery e di backup).	X	X	X	X	X		
TECH	Sicurezza Fisica	**24**	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).				X			
TECH	Sicurezza Fisica	**25**	Il Contraente deve garantire di disabilitare o di restringere l'accesso (e. g. tramite password) a qualsiasi interfaccia di prova come il JTAG (tecnologia utilizzata per il debug/emulazione di processori) sui dispositivi venduti / installati al Committente.					X	X	
TECH	Sicurezza delle comunicazioni	**26**	Il Contraente adotta protocolli di comunicazione sicuri sui propri sistemi 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. Inoltre, i flussi di 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 con algoritmo di cifratura asimmetrica, considerata ragionevolmente sicura alla data (e.g. chiave da almeno 2048 bit); - cifratura della sessione con algoritmo di cifratura simmetrico, considerato ragionevolmente sicuro alla data, con una chiave di sessione di almeno 128 bit.	X	X	X	X	X		

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Crittografia	**27**	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 deve garantire la sicurezza dei dati del Committente in transito attraverso adeguati meccanismi di cifratura. Inoltre, il Contraente deve trasmettere i dati del Committente su canali cifrati, attraverso l'utilizzo di protocolli di comunicazione sicuri (es. MTLS, HTTPS, SSH, VPN).	X	X	X	X	X		
TECH	Crittografia	**28**	Il Contraente che fornisce dispositivi IoT deve implementare gateway IoT convalidati sulla base di standard internazionali che normano i moduli crittografici (e. g. Federal Information Processing Standard Publication (FIPS) 140-2 o superiori o ISO/IEC 19790:2012)					X		
TE	Crittografia (Cloud)	**29**	Il Contraente che eroga servizi Cloud tramite servizi SaaS e PaaS dichiara quale tipo di crittografia utilizza per proteggere la riservatezza dei dati scambiati.				X			
TECH	Crittografia (Cloud)	**30**	Il Contraente che eroga servizi Cloud dichiara quale tipo di crittografia utilizza per proteggere la riservatezza dei dati archiviati presso i Data Center. Il Contraente deve formalizzare e implementare le procedure operative e i processi documentati (inclusi ruoli e responsabilità) riguardanti la gestione dei materiali crittografici (ad esempio, gestione del ciclo di vita dalla generazione della chiave alla revoca e alla sostituzione, infrastruttura della chiave pubblica, progettazione del protocollo crittografico e algoritmi utilizzati) durante il loro intero ciclo di vita, con particolare riferimento alla gestione delle chiavi (revoca e rotazione, conservazione e trasmissione sicura dei materiali della chiave, segregazione delle chiavi utilizzate per i dati o le sessioni crittografiche). Il Contraente deve garantire che le chiavi di cifratura siano in possesso esclusivo del Committente (e.g. BYOK via HSM gestito dal Committente).				X			
TECH	Network	**31**	Il Contraente deve adottare misure di sicurezza adeguate a prevenire e mitigare qualsiasi evento di sicurezza che potrebbe compromettere le funzionalità delle proprie componenti di rete tra cui, firewall, sonde IPS (i.e. Intrusion Prevention System), strumenti di analisi del traffico, limitazioni del traffico in entrata e in uscita da-verso reti non attendibili etc. Il Contraente deve implementare misure tecniche di difesa in profondità (ad es. deep packet analysis, strozzatura del traffico e black-holing) e appropriate misure di sicurezza per rilevare e rispondere tempestivamente agli attacchi di rete (es. MAC spoofing, ARP poisoning) per garantire la continuità del servizio fornito in caso di attacchi DoS (Denial of Service) in grado di avere un impatto sulla disponibilità del servizio erogato al Committente. 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.	X	X	X	X	X		
TE	Network	**32**	Il Contraente che eroga servizi Cloud assicura l'osservanza di una Policy di sicurezza delle informazioni per la configurazione delle reti virtuali VLAN.				X			

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Change Management	**33**	Il Contraente implementa un processo di Change Management per la gestione tempestiva ed efficiente di ogni cambiamento nell'ambito della propria infrastruttura, al fine di garantire che modificando il sistema del contraente non vengano impattati i dati e i sistemi del Committente.	X	X	X	X	X		
TECH	Change Management	**34**	Il Contraente 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'erogazione del servizio effettuato sull'infrastruttura del Committente. 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 Contraente deve dare comunicazione al Committente degli interventi di manutenzione attraverso un canale di comunicazione diretto.		X	X	X	X		SI
TECH	Change Management	**35**	Il Contraente che eroga servizi Cloud garantisce l'applicazione di misure di sicurezza per separare logicamente l'ambiente virtuale del Committente da quello di altri Clienti e impedire di accedere o esporre il contenuto a persone non autorizzate.				X			
TECH	Hardening	**36**	Il Contraente pone in essere apposite attività di hardening sui propri dispositivi 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.	X	X	X	X	X		
TECH	Sincronizzazione degli orologi	**37**	Tutti i sistemi cloud del Contraente utilizzano il protocollo sicuro per la sincronizzazione degli orologi. Il fuso orario utilizzato è CEST.				X			

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Documentazione di Prodotto (Hardware)	**38**	Il Contraente si impegna a fornire al Committente la documentazione tecnica di prodotto in maniera completa, accurata, coerente e aggiornata per la versione del prodotto fornita e per eventuali aggiornamenti. Tale documentazione: 1) identifica tutte le dipendenze tra i componenti, compresi quelli temporanei (es. sono documentate sia le relazioni "necessario per" che quelle "dipendente da"); 2) include un piano di manutenzione per ogni tipo di dispositivo, ad eccezione dei dispositivi che non richiedono manutenzione; 3) contiene un elenco di tutti i componenti fisici informatici (hardware inventory) come computer, controllers, RTUs, apparecchiature di rete con tutte le informazioni sul produttore, sul modello, runtime, versione del sistema operativo ecc.						X	
TECH	Documentazione di Prodotto (Software)	**39**	Il Contraente identifica e rende noti al Committente: 1) tutti i requisiti tecnici di runtime come la velocità della CPU, la dimensione della memoria, lo spazio dell'hard disk, la versione del sistema operativo; 2) Se il prodotto richiede impostazioni di configurazione specifiche, come indirizzi di rete, account utente specifici, esistenza di cartelle specifiche ecc.; 3) La documentazione del prodotto contiene un elenco di tutti i componenti software applicativi necessari per utilizzare il prodotto; 4) Tutti i prodotti software di terze parti e open source utilizzati nel prodotto sono identificati, insieme alle informazioni sul produttore e sul tipo di licenza;		X					
TECH	Documentazione di Prodotto (Hardware + Software)	**40**	Il Contraente identifica e rende noti al Committente se il prodotto comprende sia software che hardware, l'inventario del software è collegato all'inventario dell'hardware, identificando su quale hardware sono installati i programmi software documentati.		X				X	
TECH	Documentazione di Prodotto (Hardware + Software)	**41**	Il Contraente assicura che la documentazione del prodotto include una dichiarazione su eventuali "backdoor" del fornitore, ossia account e canali di accesso preconfigurati destinati all'accesso del fornitore.		X				X	

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
TECH	Documentazione di Prodotto (Hardware + Software)	**42**	Se nel prodotto sono presenti interfacce software per l'integrazione con applicazioni di terze parti, il Contraente le identifica e ne descrive brevemente tutte le funzionalità.		X				X	
ORG	Ruoli e responsabilità	**43**	Il Contraente identifica e comunica al Committente un referente per la sicurezza delle informazioni responsabile del coordinamento e del monitoraggio delle norme e procedure sulla sicurezza e che svolgerà il ruolo di interfaccia con il team di security del Committente.	X	X	X	X	X		
ORG	Gestione e utilizzo dotazioni informatiche	**44**	Relativamente ai servizi IT il Contraente applica regolamenti che tutti gli utenti con accesso ai sistemi informativi devono rispettare per il corretto utilizzo delle dotazioni informatiche aziendali, al fine di ridurre il rischio di un loro utilizzo non corretto, intenzionale o involontario, e di assicurare che il sistema informativo ed informatico del Contraente sia salvaguardato e gestito correttamente.	X	X	X	X	X		
ORG	Focal point incidenti di sicurezza	**45**	Il Contraente deve individuare un Focal Point con cui il Committente possa dialogare in caso di incidente sui sistemi del Contraente. In particolare, il Contraente deve rendere disponibile il contatto di tale Focal Point al Committente.	X	X	X	X	X		
ORG	Autorizzazione accessi	**46**	Il Contraente deve autorizzare gli accessi agli ambienti contenenti dati del Committente al proprio personale secondo i principi del "need to know" e del "least privilege", assegnando in modo univoco i diritti di accesso ad ogni user account. Il Contraente deve, dunque, definire criteri e politiche di assegnazione dei privilegi d'accesso che garantiscano l'adozione del criterio della separazione dei compiti. Per gli accessi logici il Contraente definisce una procedura interna 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 espletare le mansioni oggetto del contratto. Tali profili sono oggetto di controlli periodici. Quando l'accordo è risolto per qualsiasi ragione o è scaduto, tutti gli accessi ai dati del Committente devono essere immediatamente revocati. Tutte le informazioni e i dati del Committente in possesso del Contraente devono essere restituiti al Committente, se richiesto, e poi, salvo eventuali obblighi di legge, essere rimossi e cancellati in modo sicuro (p.e. wiping) dai dispositivi del Contraente.	X	X	X	X	X		

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
ORG	IAM	**47**	Il Contraente, nel caso di erogazione di servizi applicativi che prevedono l'utilizzo di credenziali di accesso ai sistemi del Committente, deve garantire l'integrazione con il sistema di Identity e Access Management del Committente in modo tale da permettere al Committente di gestire l'autenticazione e i profili di accesso degli utenti.		X	X	X			SI
ORG	Provisioning e Deprovisioning utenze	**48**	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.	X	X	X	X	X		
ORG	Gestione interventi di assistenza IT	**49**	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 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 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.		X	X	X	X		

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
ORG	Gestione interventi di assistenza IT	**50**	Il Contraente che eroga servizi Cloud fornisce al Committente un servizio di assistenza e supporto tecnico con costi e orari di servizio definiti. Il Contraente deve dichiarare gli obiettivi corrispondenti agli indicatori di qualità del servizio sotto riportati e garantirne 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 Committente 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 Committente 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.)				X			

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
ORG	Change Management	**51**	Il Contraente deve applicare 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 e la tutela dei 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).	X	X	X	X	X		
ORG	Change Management	**52**	Il Contraente che deve apportare delle modifiche o dei cambiamenti nei sistemi del Committente deve rispettare i requisiti di sicurezza e le procedure definite dal Committente per assicurare che rispetti e implementi tutte le misure di sicurezza tecnico-organizzative volte ad attuare in modo efficace i principi di protezione dei dati personali e 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).		X	X		X		SI
ORG	Sviluppo sicuro e test per servizi Hardware	**53**	Il contraente che fornisce dispositivi hardware deve garantire un'analisi continua delle vulnerabilità tecniche del prodotto. Notificando al contraente eventuali vulnerabilità riscontrate.						X	
ORG	Sviluppo sicuro e test per servizi IT	**54**	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, pertanto, deve integrare i processi e gli strumenti per il Secure Software Development Lifecycle (SDLC) con controlli / requisiti di sicurezza appropriati (es. Source Code Security Analysis). Il test del codice segue un processo predefinito finalizzato a valutare sia la funzionalità del codice sia la presenza di vulnerabilità gravi. L'iter approvativo per il passaggio in produzione viene opportunamente tracciato. Tutti i test effettuati, i risultati ed eventuali piani di rimedio devono essere tracciati su un apposito registro custodito in sicurezza. Gli ambienti di sviluppo, test e produzione sono fisicamente e logicamente separati.		X	X	X	X		

				TIPOLOGIA DI FORNITURA						
Ambito	**Categoria**	**ID**	**Clausole di sicurezza**	**Professional Services**	**Application Development Services**	**Application Management Services**	**Cloud Services**	**Infrastructure & system maintenance**	**Hardware Procurement**	**Applicabile ai Sistemi ASPI**
ORG	Formazione	**55**	Il Contraente eroga periodicamente ai propri dipendenti coinvolti nelle attività di 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.	X	X	X	X	X		
ORG	Audit Interni	**56**	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.	X	X	X	X	X		