	versione 1.2 aprile 2025
ISTRUZIONI PER LA COMPILAZIONE	
ANAGRAFICA	L'anagrafica va compilata in ogni sua parte
ANAGRAFICA - PERIODO DI RIFERIMENTO	E' il periodo a cui si riferiscono le risposte del questionario. I campi "dal" "al" vanno valorizzati con le rispettive date nel formato gg/mm/aaaa.
QUESTIONARIO- COLONNE SI - NO - N/A	Tutte le domande del questionario prevedono una risposta attraverso la valorizzazione dei campi "SI", "NO" o "N/A" con una "X" nella colonna di interesse. Non devono essere lasciate domande senza risposta.
QUESTIONARIO - UTILIZZO DELLA COLONNA N/A	Il campo N/A deve essere valorizzato esclusivamente in caso di fattispecie non applicabile.
QUESTIONARIO- SEZIONE M - RICORSO AD ALTRO RESPONSABILE (di seguito SUB-RESPONSABILE)	La sezione deve essere compilata unicamente qualora il Responsabile ricorra ad uno o più altri responsabili (sub-responsabili) e deve essere ripetuta con riferimento ad ogni altro responsabile nominato.
QUESTIONARIO- FOGLIO DENOMINATO "SEZ. SOGG. ART. 1, L. 90/2024 "	La sezione Y è stata inserita in un foglio separato in quanto deve essere compilata esclusivamente dai soggetti che rientrano nell' ambito di applicazione dell'articolo 1 , comma 1, della Legge 28 giugno 2024, n. 90

ACRONIMI	
RPD o DPO	Responsabile Protezione Dati o Data Protection Officer
RGPD	REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI Reg. UE 2016/679
ADS	Amministratore di sistema

QUESTIONARIO PER LA VERIFICA DEL RISPETTO DEL REGOLAMENTO (UE) 2016/679 "*REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI*" SULLE ATTIVITA' DI TRATTAMENTO DA PARTE DEL RESPONSABILE DEL TRATTAMENTO

PERIODO DI RIFERIMENTO	
DAL	GG/MM/AAAA
AL	GG/MM/AAAA

NOME E COGNOME O RAGIONE SOCIALE O DENOMINAZIONE SOCIALE DEL RESPONSABILE DEL TRATTAMENTO	
CODICE FISCALE/PARTITA IVA	
NOME E COGNOME DEL LEGALE RAPPRESENTANTE	
DATA DI SOTTOSCRIZIONE DELL'ATTO DI DESIGNAZIONE	
NOME E COGNOME E DATI DI CONTATTO DEL RESPONSABILE DELLA PROTEZIONE DATI (RPD o DPO)	

				versione 1.2 aprile 2025
A	**ASPETTI GENERALI**	**SI**	**NO**	**N/A**
A1	Sono state/sono effettuate le operazioni di trattamento nel rispetto delle disposizioni operative del Titolare?			
A2	Sono stati/sono effettuati trattamenti su dati personali diversi rispetto a quelli normalmente eseguiti nell'ambito della designazione?			
A2.1	In caso di risposta affermativa alla domanda A2, si è provveduto, all'insorgere dell'esigenza, ad informare preventivamente il Titolare del trattamento e il RPD della Regione Lazio?			
A3	Sono stati/sono effettuati trattamenti su dati personali diversi rispetto a quelli normalmente eseguiti nell'ambito della designazione?			
B	**REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO**	**SI**	**NO**	**N/A**
B1	E' stato presidposto il registro delle attività di trattamento svolte per conto del Titolare, in forma scritta, anche in formato elettronico, da esibire in caso di verifiche e/o ispezioni del Titolare o dell'Autorità?			
B2	Il Registro contiene le seguenti informazioni:			
B2.1	il nome e i dati di contatto del responsabile o dei responsabili del trattamento, del titolare del trattamento per conto del quale agisce il responsabile del trattamento e, ove nominato, del RPD			
B2.2	le categorie/attività dei trattamenti effettuati			
B2.3	i trasferimenti di dati personali verso Paesi terzi o organizzazioni al di fuori dello Spazio Economico Europeo, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del RGPD, la documentazione delle garanzie adeguate;			
B2.4	ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.			
B3	Il Registro viene regolarmente aggiornato?			
C	**RPD DEL RESPONSABILE DEL TRATTAMENTO**	**SI**	**NO**	**N/A**
C1	E' stato designato un RPD?			
C2	In caso di risposta affermativa:			
C2.1	Il RPD è stato designato con atto formale?			
C2.3	I dati ed i punti di contatto del RPD sono stati comunicati al Titolare?			
D	**SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI**	**SI**	**NO**	**N/A**
D1	Sono stati designati i soggetti autorizzati al trattamento dati all'interno della struttura?			
D2	In caso di risposta affermativa alla domanda D1:			
D2.1	sono stati autorizzati con atto formale?			
D2.2	sono stati adeguatamente istruiti sul tema della protezione dei dati personali?			
D2.3	sono previste attività formative con aggiornamenti periodici in tema di protezione di dati personali?			
D2.4	le istruzioni operative impartite ai soggetti autorizzati sono idonee a garantire il rispetto delle finalità per cui i dati sono stati raccolti, e trattati?			
D2.5	i soggetti autorizzati al trattamento sono vincolati ad un obbligo, legalmente assunto, di riservatezza?			
D3	Alcune attività vengono svolte in modalità di "lavoro agile"?			
D4	Il "lavoro agile" è disciplinato da regolamenti e/o procedure interne?			
E	**AMMINISTRATORI DI SISTEMA**	**SI**	**NO**	**N/A**
E1	Sono stati individuati i soggetti ai quali affidare il ruolo di Amministratori di Sistema (*System Administrator*), Amministratori di Base Dati (*Database Administrator*), Amministratori di Rete (*Network Administrator*) e/o Amministratori di *Software* complessi?			
E2	In caso di risposta affermativa alla domanda E1:			
E2.1	Sono stati sottoscritti appositi atti di designazione individuale?			
E2.2	Sono state impartire adeguate istruzioni ai designati secondo i ruoli assegnati?			
E2.3	Sono state adottate adeguate misure di controllo e di vigilanza sul loro operato?			
E2.4	E' stato aggiornato l'elenco degli ADS con l'indicazione delle relative utenze?			
E2.5	Le nomine degli Amministratori sono aggiornate ad ogni modifica della normativa vigente?			
E3	È stata assegnata ai suddetti soggetti una *user id* agevolmente riconducibile all'identità degli Amministratori?			
E4	In caso di risposta affermativa alla domanda E3 sono rispettate le seguenti regole?			
E4.1	divieto di assegnazione di *user id* generiche e già attribuite anche in tempi diversi;			
E4.2	utilizzo di utenze amministrative anonime, quali "*root*" di *Unix o* "*Administrator*" di *Windows*, solo per situazioni di emergenza;			
E4.3	le credenziali utilizzate assicurano sempre l'imputabilità delle operazioni a chi ne fa uso;			
E4.4	disattivazione delle *user id* attribuite agli Amministratori che, per qualunque motivo, non necessitano più di accedere ai dati.			
E5	Le password associate alle *user id* assegnate agli Amministratori prevedono il rispetto delle seguenti regole?			
E5.1	*password* con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata;			
E5.2	cambio *password* alla prima connessione e successivamente almeno ogni 30 giorni (*password again*);			
E5.3	le *password* devono differire dalle ultime 5 utilizzate (*password history*);			
E5.4	le *password* sono conservate in modo da garantirne disponibilità e riservatezza;			
E5.5	registrazione di tutte le immissioni errate di *password*;			
E6	Gli *account* degli Amministratori sono bloccati dopo un numero massimo di tentativi falliti di *login*, ove tecnicamente possibile?			
E7	L'archiviazione di *password* o codici PIN, su qualsiasi supporto fisico avvenga, è protetta da sistemi di cifratura?			

E8	È assicurata la completa distinzione, in capo al medesimo utente, tra utenze privilegiate (amministratore) e non privilegiate, alle quali devono corrispondere credenziali diverse?			
E9	I profili di accesso per le utenze di ADS rispettano il principio del *need-to-know*, ovvero che non siano attribuiti diritti oltre a quelli realmente necessari per eseguire le attività di lavoro?			
E10	I sistemi sono dotati di strumenti automatici tipo *alert* che si attivano ad esempio quando viene aggiunta una utenza amministrativa e/o quando sono aumentati i diritti di una utenza amministrativa già attiva?			
E11	Sono stati adottati sistemi di registrazione degli accessi logici (*log*) degli Amministratori ai sistemi?			
E12	La conservazione dei registri degli accessi logici è garantita per un periodo non inferiore a 6 mesi?			
E13	In caso di utilizzo di sistemi messi a disposizione dalla Regione, è stato comunicato agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei *log*?			
E14	Sono state adottate idonee misure finalizzate ad obbligare l'Amministratore ad accedere ai sistemi con una utenza normale e solo successivamente eseguire i singoli comandi come ADS?			
E15	Sono stati comunicati al momento della sottoscrizione dell'atto di designazione e con cadenza almeno annuale o ogni qualvolta se ne verifichi la necessità alla Regione Lazio gli estremi identificativi dei soggetti nominati Amministratori di Sistema?			
E16	Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?			
E17	Sono state adottate idonee misure per consentire di mettere a disposizione del Titolare e del RPD della Regione Lazio le informazioni relative ai *log* delle operazioni per un periodo di 6 mesi, qualora necessario?			
F	**PRIVACY BY DESIGN E BY DEFAULT**	**SI**	**NO**	**N/A**
F1	Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (*privacy by design*)?			
F2	È stato adottato sistema di monitoraggio delle politiche aziendali di *privacy by design* e *by default* affinchè le stesse possano adeguarsi ai mutamenti tecnologici e all'insorgere di nuovi rischi?			
F3	Sono state eseguite le valutazioni del rischio per ciascun trattamento?			
F4	Sono state strutturate le operazioni in modo da minimizzare il trattamento dei dati personali?			
F5	Sono state adottate tutte le misure necessarie per perseguire la massima trasparenza dei trattamenti di dati personali rendendo accessibile agli interessati idonea documentazione?			
G	**MISURE DI SICUREZZA**	**SI**	**NO**	**N/A**
G1	Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?			
G2	I soggetti di cui alla domanda G1 agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali?			
G3	Sono state messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio?			
G4	In caso di risposta affermativa alla domanda G3, le misure adottate comprendono:			
G4.1	la pseudonimizzazione e/o la cifratura dei dati personali?			
G4.2	misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?			
G4.3	misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?			
G4.4	procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento?			
G5	Sono state predisposte misure tecniche che consentono l'accesso ai dati personali unicamente ai soggetti autorizzati?			
G6	Sono state adottate almeno le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID del 18 aprile 2017, n. 2/2017?			
G7	È stata prediposta idonea documentazione tecnica relativa alle misure di sicurezza in atto?			
G8	In caso di risposta affermativa alla domanda G7:			
G.8.1	la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto?			
G.8.2	la documentazione è disponibile e producibile a richiesta del Titolare?			
G9	È stato adottato un approccio alla sicurezza dei dati basato sul rischio?			
G10	È presente un impianto antintrusione?			
G11	Sono presenti procedure di controllo per l'accesso dei visitatori?			
G12	È prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?			
G13	Gli operatori autorizzati possono accedere ai dati trattati con strumenti informatici soltanto dopo almeno uno o due processi di autenticazione (ad esempio il primo accesso al sistema operativo e il secondo accesso all'applicativo specifico)?			
G14	Gli operatori autorizzati utilizzano credenziali di accesso individuali?			
G15	Gli operatori autorizzati utilizzano dispositivi personali (PC portatili, tablet, smartphone, etc) per il trattamento dei dati?			
G16	L'accesso ai collegamenti VPN avviene dopo l'autenticazione a due fattori di cui uno è OTP?			
G17	È presente una procedura interna, nel caso sia permesso ai soggetti autorizzati l'utilizzo di risorse informatiche (es. PC, Tablet, smartphone) di proprietà di terzi?			
G18	I sistemi informativi sono gestiti in proprio?			
G19	In caso di risposta affermativa alla domanda G18:			
G19.1	è installato sui dispositivi un sistema antivirus e *antimalware* aggiornato?			
G19.2	sono conservati i dati in *tenant* diversi e separati per ciascun Titolare che li ha rispettivamente forniti?			
G19.3	è aggiornato costantemente il Sistema Operativo installato sugli elaboratori elettronici?			
G19.4	è prevista una mappatura del proprio sistema informatico (hardware, software, dati, procedure)?			
G19.5	è presente un Piano di Continuità Operativa?			
G19.6	è effettuato con cadenza temporale programmata un test sul Piano di Continuità Operativa?			

G19.7	è presente un Piano di *Disaster Recovery*?			
G19.8	è effettuata con cadenza temporale programmata *penetration test* sul sistema di elaborazione dei dati?			
G19.9	è presente un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di elaborazione e conservazione dei dati?			
G19.10	è presente un impianto antintrusione?			
G19.11	sono presenti delle procedure per l'acceso controllato dei visitatori?			
G19.12	sono presenti dei sistemi di valutazione interni delle misure di sicurezza?			
G19.13	sono presenti i sistemi a valutazione esterna (certificazione)?			
G19.14	sono stati adottati i sistemi di crittografia per proteggere i dati memorizzati?			
G19.15	sono stati adottati i sistemi di crittografia per proteggere i dati in transito?			
G19.16	è presente un SOC?			
G19.17	è presente un sistema SIEM?			
G19.18	è prevista una regolare formazione degli operatori sui temi dell'utilizzo sicuro del Sistema?			
G19.19	sono protette le connessioni ad Internet con sistemi di *firewall*, *intrusion detenction sistem* ecc.?			
G19.20	Sono in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni tecniche o di compatibilità con sistemi *legacy*)?			
G19.21	nell'ambito di test di sviluppo del software, sono usati dati anonimizzati?			
G19.22	sono utilizzati ambienti di sviluppo software, test, collaudo e di produzione fisicamente e logicamente separati?			
G20	I sistemi utilizzati sono gestiti da terzi?			
G21	In caso di risposta affermativa alla domanda G20 si è certi che il soggetto terzo:			
G21.1	abbia installato sui dispositivi un sistema antivirus e antimalware aggiornato?			
G21.2	conservi i dati in tenant diversi e separati per ciascun Titolare che li ha rispettivamente forniti?			
G21.3	provveda ad aggiornare costantemente il Sistema Operativo installato sugli elaboratori elettronici?			
G21.4	disponga di una mappatura del proprio sistema informatico (hardware, software, dati, procedure)?			
G21.5	disponga di un Piano di Continuità Operativa?			
G21.6	effettui con cadenza temporale programmata test sul Piano di Continuità Operativa?			
G21.7	disponga di un Piano di Disaster Recovery?			
G21.8	effettui con cadenza temporale programmata penetration test sul sistema di elaborazione dei dati?			
G21.9	sia dotato di un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di elaborazione e conservazione dei dati?			
G21.10	sia dotato di impianto antintrusione?			
G21.11	sia dotato di procedure per l'acceso controllato dei visitatori?			
G21.12	sia dotato di sistemi di valutazione interni delle misure di sicurezza?			
G21.13	sottoponga i istemi a valutazione esterna (certificazione)?			
G21.14	abbia adottato sistemi di crittografia per proteggere i dati memorizzati?			
G21.15	abbia adottato sistemi di crittografia per proteggere i dati in transito?			
G21.16	sia dotato di un SOC?			
G21.17	sia dotato di un sistema SIEM?			
G21.18	proceda alla regolare formazione degli operatori sui temi dell'utilizzo sicuro del Sistema?			
G21.19	protegga le connessioni ad Internet con sistemi di firewall, intrusion detenction sistem ecc.?			
G21.20	non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni tecniche o di compatibilità con sistemi legacy)?			
G21.21	nell'ambito di test di sviluppo del software, usi dati anonimizzati?			
G21.22	utilizzi ambienti di sviluppo software, test, collaudo e di produzione fisicamente e logicamente separati?			
H	**PROCEDURE DI GESTIONE DEL SISTEMA INFORMATIVO AZIENDALE**	**SI**	**NO**	**N/A**
H1	Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?			
H2	In caso di risposta affermativa alla domanda H1:			
H2.1	è conforme a standard internazionali?			
H2.2	prevede regole per la gestione delle credenziali di accesso ai database?			
H2.3	prevede regole per la gestione delle password e per l'accesso alle applicazioni?			
H2.4	prevede regole per la gestione degli accessi ad Internet?			
H2.5	prevede regole per la gestione degli accessi a *social media* (es: *Facebook*, *You Tube, Twitter* ecc)?			
H2.6	prevede regole per la gestione e l'utilizzo della posta elettronica?			
H2.7	prevede regole per la gestione dei diritti di accesso ai dati?			
H2.8	prevede regole per la gestione degli incidenti informatici?			
H2.9	prevede regole per l'assistenza agli utenti?			
H2.10	prevede regole per la protezione antivirus?			
H2.11	prevede regole per la gestione dei dispositivi mobili utilizzati per il trattamento dei dati (PC portatili, smartphone, tablet, chiavi USB, dischi esterni di memorizzazione dei dati?			
H2.12	prevede regole per autorizzare i dipendenti a trasferire, archiviare o trattare dati personali al di fuori dei locali dell'organizzazione?			
H2.13	prevede regole per il salvataggi di backup dei dati?			
H2.14	prevede regole per la gestione delle stampe protette?			
H2.15	prevede regole per la custodia e gestione degli archivi cartacei?			
I	***DATA BREACH***	**SI**	**NO**	**N/A**
I1	È stata adottata una procedura per la gestione delle violazioni di dati personali (*data breach*)?			
I2	Sono state predisposte misure organizzative idonee a garantire la tempestiva informazione al Titolare ed al RPD della Regione Lazio, (entro 24 ore dall'avvenuta conoscenza dell'evento), di ogni violazione di dati personali (*data breach*)?			

I3	Sono state adottate misure organizzative idonee a garantire che l'informazione sulla violazione dei dati personali (*data breach*), sia corredata da tutta la documentazione utile per permettere al Titolare la tempestiva valutazione sulla necessità di notifica di violazione all'Autorità Garante per la protezione dei dati personali e/o di comunicazione agli interessati, entro i termini stabiliti dal RGPD?			
I4	Sono stati subiti attacchi informatici con violazione di dati personali?			
I5	Sono stati notificati nell'ultimo anno violazioni di dati personali al Garante?			
L	**VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI**	**SI**	**NO**	**N/A**
L1	Sono state adottate misure tecniche ed organizzative idonee a garantire adeguata assistenza al Titolare nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD, qualora lo stesso ne faccia richiesta?			
M	**RICORSO AD ALTRO RESPONSABILE (di seguito SUB-RESPONSABILE)**	**SI**	**NO**	**N/A**
M1	È stato effettuato ricorso ad altro/i responsabile/i (sub-responsabili) per gestire le attività di trattamento?			
M2	In caso di risposta affermativa alla domanda M1:			
M2.1	è stata rilasciata autorizzazione scritta, specifica o generale, del Titolare del Trattamento?			
M2.1.1	In caso di autorizzazione specifica, è stato/a indicato/a:			
M2.1.2	quale sub responsabile sia autorizzato?			
M2.1.3	la durata dell'autorizzazione?			
M2.1.4	la specifica attività di trattamento?			
M2.2	E' costantemente aggiornato l'elenco dei sub responsabili conformemente all'autorizzazione generale o specifica rilasciata dal Titolare?			
M2.3	E' stato informato il Titolare del trattamento di eventuali modifiche all'elenco originario dei sub-responsabili?			
M2.4	La nomina del sub-responsabile è avvenuta mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri contenente gli stessi obblighi in materia di protezione dei dati contenuti nel contratto (o in altro atto giuridico) tra il Titolare del trattamento e il Responsabile del trattamento?			
M2.5	I contratti sottoscritti con i sub-responsabili sono conformi ai principi e ai contenuti normativamente prescritti (cfr. par. 70 EDPB_Opinion 22/2024)?			
M2.6	E' sempre garantita la disponibilità delle copie dei contratti sottoscritti con i sub-responsabili per eventuali richieste del Titolare del trattamento?			
M2.7	Nel contratto (o altro atto giuridico) di nomina è stato previsto che il sub-responsabile fornisca sufficienti garanzie per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD?			
M2.8	Il sub-responsabile nominato detiene un registro con le medesime caratteristiche formali ed i medesimi contenuti sopra indicati relativamente ai trattamenti di competenza?			
M2.9	Nel contratto/altro atto giuridico sono state fornite adeguate istruzioni al sub-responsabile?			
M2.10	Le informazioni necessarie all'identificazione dei sub-responsabili (es. nome, indirizzo, contatto) sono disponibili per essere fornite al titolare in caso di richiesta, in ottempereranza all'obbligo di cui all'art. 28 par. 3 lettera h) del GDPR (cfr. *par.* 32 EDPB_Opinion 22/2024)?			
M2.11	Sono state effettuate periodiche verifiche sull'adeguatezza delle misure tecniche e organizzative adottate dal sub-responsabile?			
M2.12	Il sub-responsabile si attiene alla sua politica di sicurezza con particolare riferimento all'accesso ai dati dell'amministrazione?			
N	**CANCELLAZIONE E/O RESTITUZIONE DEI DATI PERSONALI TRATTATI**	**SI**	**NO**	**N/A**
N1	Sono state adottate misure tecniche ed organizzative idonee a garantire la cancellazione o la restituzione di tutti i dati personali nei termini stabiliti per la prestazione dei servizi o, comunque, a richiesta del Titolare?			
N2	È presente una procedura operativa per la dismissione dei supporti dei dati?			
N3	Sono presenti i dispositivi per la distruzione dei documenti cartacei?			
O	**TRASFERIMENTO DI DATI PERSONALI VERSO UN PAESE TERZO O UN'ORGANIZZAZIONE INTERNAZIONALE**	**SI**	**NO**	**N/A**
O1	Vengono effettuati trasferimenti di dati personali verso Paesi terzi o organizzazioni al di fuori dello Spazio Economico Europeo?			
O2	In caso di risposta affermativa alla domanda O1:			
O2.1	è stata ottenuta l'autorizzazione scritta da parte del Titolare?			
O2.2	sono state adottate idonee misure per il rispetto del Capo V (artt. 44 - 50) del RGPD?			
O2.3	è stata effettuata una mappatura dei trasferimenti? (cfr. nota 57 EDPB_Opinion 22/2024)			
O2.3.1	In caso di risposta affermativa alla domanda O 2.3, la mappatura comprende:			
O2.3.2	l'indicazione dei dati trasferiti?			
O2.3.3	le finalità del trasferimento?			
O2.3.4	la norma che legittima il trasferimento?			
O2.4	sono state adottate misure tecniche ed organizzative idonee a garantire adeguata assistenza al Titolare nello svolgimento della valutazione d'impatto sul trasferimento dei dati?			
P	**CODICI DI CONDOTTA E CERTIFICAZIONI**	**SI**	**NO**	**N/A**
P1	E' prevista l'adesione a un codice di condotta ai sensi dell'art. 40 del RGPD?			
P2	Si è in possesso della certificazione ISDP©10003 (ITA)?			
P3	Si è in possesso della certificazione Carpa (LU)?			
P4	Si è in possesso della certificazione Europrivacy (LU)?			
P5	Si è in possesso della certificazione Europrice (D)?			
P6	Si è in possesso della certificazione accreditata IS0 17065 in materia di protezione dei dati personali?			
P7	Si è in possesso della certificazione ISO 9001?			

P8	Si è in possesso della certificazione ISO 27001?			
P9	Si è in possesso della certificazione ISO 22301?			
P10	Si è in possesso della certificazione ISO 20000-1?			
P11	Si è in possesso della certificazione ISO 27701?			
P12	Si è in possesso della certificazione ISO/IEC 27017 e ISO/IEC 27018, integrate, come addendum alla Norma ISO/IEC 27001?			
P13	Si è in possesso di altra certificazione accreditata (e/o integrata) come addendum alla Norma ISO/IEC 27001?			
P14	Si è in possesso di altra certificazione accreditata in materia di privacy e gestione della sicurezza delle informazioni?			
P15	E' presente la certificazione rilasciata da organismi di certificazione di cui all'articolo 43 del RGPD o dall'autorità di controllo, come previsto dall'art. 42 del RGPD, che dimostri la conformità al RGPD?			
Q	**ESERCIZIO DEI DIRITTI DEGLI INTERESSATI**	**SI**	**NO**	**N/A**
Q1	Sono state adottate procedure atte a consentire l'esercizio dei diritti degli interessati?			
Q2	In caso di risposta affermativa alla domanda Q1 sono previste procedure per:			
Q2.1	la limitazione del trattamento?			
Q2.2	la portabilità dei dati?			
Q2.3	la cancellazione dei dati su richiesta dell'interessato?			
Q2.4	la cancellazione dei dati al termine del periodo previsto?			
Q2.5	l'estrazione dei dati su richiesta dell'interessato?			
Q2.6	la rettifica dei dati?			
Q2.7	la gestione dell'opposizione al trattamento?			
Q3	Sono state adottate misure tecniche ed organizzative idonee ad assistere il Titolare nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD?			
Q4	Sono state ricevute istanze degli interessati in esercizio ai diritti di cui agli articoli da 15 a 22 del RGPD?			
Q5	In caso di risposta affermativa alla domanda Q4:			
Q5.1	è stata effettuata tempestiva comunicazione scritta al Titolare e al RPD della Regione Lazio, allegando copia della richiesta?			
Q5.2	è stato effettuato il coordinamento con il Titolare e con il RPD della Regione Lazio al fine di soddisfare le richieste?			
R	**FUNZIONI CRITTOGRAFICHE - CONSERVAZIONE DELLE PASSWORD**	**SI**	**NO**	**N/A**
R1	È utilizzato un sistema di autenticazione federato (es. LDAP, Spid, ecc.)?			
R2	In caso di risposta negativa alla domanda R1:			
R2.1	Sono state adottate le misure tecniche previste nelle *Linee Guida Funzioni Crittografiche – Conservazione delle Password* approvate con provvedimento del Garante registro n. 594 del 7 dicembre 2023 al fine di proteggere in modo efficace le password e conservarle nell'ambito di sistemi di autenticazione informatica, o di altri sistemi, secondo le istruzioni impartite dal Titolare?			
R3	In caso di risposta affermativa alla domanda R2.1:			
R3.1	Sono state adottate totalmente le misure tecniche previste?			
R3.2	Sono state adottate parzialmente le misure tecniche previste?			
R3.3	Sono state fornite idonee istruzioni agli Amministratori di sistema?			
R3.4	Sono state fornite idonee istruzioni ai sub-responsabili ove nominati?			
R3.5	In caso di affidamenti di nuovi servizi, è stato previsto previsto l'inserimento di apposite clausole nei capitolati tecnici di gara?			
R4	In caso di risposta negativa alla domanda R2.1:			
R4.1	La circostanza è stata comunicata al Titolare del trattamento?			
R4.2	È possibile comprovare che le misure tecniche adottate garantiscano comunque un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche?			
R4.3	nel determinare il periodo di conservazione delle password, è previsto l'adeguamento alle indicazioni sui criteri da utilizzare fornite dal Garante nel provvedimento registro n. 594 del 7 dicembre 2023?			
R4.4	le password sono tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per verificare l'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online?			
R4.5	le password sono tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per garantirne la sicurezza dei sistemi informatici o servizi online?			
R4.6	le password sono tempestivamente cancellate, anche in modo automatico in caso di cessazione dei sistemi informatici o servizi online?			
R4.7	le password sono tempestivamente cancellate, anche in modo automatico in caso di disattivazione delle relative credenziali di autenticazione?			
S	**REQUISITI GENERALI DI SICUREZZA (Linee Guida Agid_ Sicurezza nel procurement ICT)**	**SI**	**NO**	**N/A**
S1	È effettuato annualmente un audit sul sistema di sicurezza da una società specializzata scelta previa approvazione della stazione appaltante?			
S2	Il personale che presta supporto operativo nella sicurezza, possiede le necessarie certificazioni?			
S3	Sono condivise le informazioni necessarie per il monitoraggio della qualità e della sicurezza?			
S4	In caso di risposta affermativa alla domanda S3:			
S4.1	Sono state pubblicate dette informazioni all'interno del portale della fornitura?			
S5	È stata sottoscritta una clausola di non divulgazione (NDA) relativa ai dati e alle informazioni dell'Amministrazione Appaltante?			
S6	Le soluzioni e i servizi di sicurezza proposti sono aggiornati da un punto di vista teconologico?			
S7	Le soluzioni e i servizi di sicurezza proposti sono conformi alle normative e agli standard di riferimento?			
S8	Le soluzioni e i servizi di sicurezza proposti sono adattabili alle normative future senza oneri aggiuntivi?			

T	REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI SVILUPPO APPLICATIVO	SI	NO	N/A
T1	Sono effettuate forniture di servizi di sviluppo applicativo?			
T2	In caso di risposta affermativa alla domanda T1:			
T2.1	In fase di progettazione e codifica, sono implementate le specifiche di sicurezza nel codice e nella struttura della base dati, con particolare riferimento alle "Linee Guida per lo sviluppo del software sicuro" di AgID?			
T3	È stata rilasciata tutta la documentazione necessaria all'Amministrazione al termine del progetto, incluso quanto riguarda la sicurezza?			
U	**REQUISITI SPECIFICI PER FORNITURE DI OGGETTI CONNESSI IN RETE**	**SI**	**NO**	**N/A**
U1	Sono effettuate forniture di oggetti connessi in rete?			
U2	In caso di risposta affermativa alla domanda T1:			
U2.1	Sono utilizzati protocolli sicuri e cifrati (HTTPS,SSH v2, ecc.)?			
U2.2	È effettuato il filtraggio degli inidrizzi IP?			
U2.3	Sono offerti processi, unità organizzative e strumenti dedicati alla gestione delle vulnerabilità scoperte sui prodotti oggetto della fornitura?			
V	**REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI GESTIONE REMOTA**	**SI**	**NO**	**N/A**
V1	Sono effettuate forniture di servizi di gestione remota?			
V2	In caso di risposta affermativa alla domanda V1			
V2.1	Sono utilizzati meccanismi che permettano di garantire l'integrità di quanto trasmesso?			
V3	In caso di necessità, da parte degli operatori, di accesso a Internet, è utilizzato un proxy centralizzato e dotato di configurazione?			
V4	Su richiesta dell'amministrazione, è effettuata la consegna alla stessa dei log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT?			
V5	In caso di risposta affermativa alla domanda V4			
V5.1	Sono inviati i log all'amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta?			
V6	è monitorata la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite?			
Z	**REQUISITI SPECIFICI IN CASO DI ADOZIONE DI SOFTWARE GESTIONALI ("Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale" , approvato con Provvedimento del Garante per la Protezione dei Dati Personali n. 618 del 17 ottobre 2024 e pubblicato sulla Gazzetta Ufficiale Serie Generale n. 278 del 27 novembre 2024).**	**SI**	**NO**	**N/A**
Z1	Sono utilizzati software gestionali per la gestione dei trattamenti?			
Z2	Il produttore del software ha aderito al Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale adottato con Provvedimento del Garante per la Protezione dei Dati Personale n. 618 del 17 ottobre 2024?			
Z3	In caso di risposta affermativa alla domanda Z2 passare direttamente alla sezione successiva (sezione X)			
Z4	In caso di risposta negativa alla domanda Z2, è stato verificato che:			
Z4.1	i dati personali raccolti sono solo quelli necessari rispetto alle finalità individuate?			
Z4.2	i dati personali sono trattati solo da coloro che ne hanno effettiva necessità?			
Z4.3	i dati personali sono trattati solo per il tempo strettamente necessario per il perseguimento della finalità?			
Z4.4	sono documentati gli strumenti utilizzati per trattare i dati (indicazione del DB, strumento di cattura del codice, sistema di conservazione dei doc. prodotti)?			
Z4.5	sono definite le misure di sicurezza a tutela dei dati?			
Z4.6	sono utilizzate utenze nominative individuali per garantire la tracciabilità delle operazioni eseguite?			
Z4.7	le password policy sono conformi alle best practice europee e internazionali di riferimento (es. minimo 8 caratteri, presenza di caratteri speciali, scadenza, ciclicità)?			
Z4.8	sono adottate misure per prevenire e contrastare attacchi informatici (credential stuffing, brute force, passowrd spraying?			
Z4.9	è implementata l'autenticazione a più fattori (MFA) in base al livello di rischiosità dei dati personali?			
Z4.10	sono adottate delle misure che consentono di monitorare e gestire i rischi inerenti agli accessi ai sistemi applicativi (es. disattivazione credenziali in caso di inutilizzo per tempi prolungati ecc.)?			
Z4.11	sono utilizzate misure di autenticazione per le API (es. certificati digitali o token)?			
Z4.12	gli utenti accedono solo a funzioni, file di dati, URL, per cui sono espressamente autorizzati?			
Z4.13	sono adottate tecniche di pseudonimizzazione o cifratura dei dati personali (tokenizzazione, ecc.)?			
Z4.14	sono utilizzate tecniche crittografiche adeguate per la conservazione delle password degli utenti (es. Key Derivation Function)?			
Z4.15	lo sviluppo degli applicativi è effettuato in linea con le policy e procedure adottate?			
Z4.16	in caso di software esposto su reti pubbliche, sono effettuati test di penetrazione periodici?			
Z4.17	sono effettuate analisi di vulnerabilità a cadenza periodica?			
Z4.18	è effettuata l'integrazione di funzionalità per il tracciamento dei log degli accessi e delle attività svolte in relazione ai diversi tipi di utenza (log applicativi di attività utente) allo scopo di consentire il monitoraggio?			
Z4.19	è prevista la separazione degli ambienti di test e sviluppo rispetto agli ambienti di produzione?			
Z4.20	ove ne ricorrano i presupposti, in caso di esercizio del diritto alla portabilità da parte dell'interessato, sono integrate funzionalità idonee a consentire l'estrazione dei dati personali in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo?			
Z4.21	il software gestionale consente di impostare (*di default*) la cancellazione dei dati personali trascorso il periodo necessario di conservazione?			
Z4.22	sono effettuate periodiche sessioni formative al personale autorizzato al trattamento dei dati personali?			
Z4.23	è conservato un inventario delle componenti software in uso, comprese le librerie di terzi e/o open source (SBOM - Software Bill of Materials)?			

Z4.24	è regolamentato il processo di gestione delle modifiche applicative ed infrastrutturali (Change management)?			
Z4.25	è regolamentato il processo di Configuration management per la gestione delle versioni dei rilasci dei moduli software?			
Z4.26	il software gestionale include funzionalità per il backup dei dati trattati?			
Z4.27	sono adottate misure per assicurare l'esattezza e l'accuratezza dei dati trattati (es. controlli di correttezza formale della PIVA o CF)?			
Z4.28	sono adottate misure per garantire la riservatezza dei dati in caso di utilizzo di funzioni di condivisione dei dati (es. invio di avvisi o notifiche)?			
Z4.29	sono utilizzati protocolli sicuri per proteggere i dati durante la loro trasmissione (protocolli crittografici standard)?			
Z4.30	sono integrate le funzionalità per l'eliminazione dei file temporanei contenenti dati personali e la cancellazione sicura dei dati sugli strumenti dismessi?			
Z5	Sono adottati software gestionali on premise?			
Z5.1	In caso di risposta affermativa alla domada Z5, è stato verificato che:			
Z5.2	sono rispettati tutti i requisiti di autorizzazione ed autenticazione degli operatori alle piattaforme utilizzate per l'assistenza (es. accesso previa autenticazione, blocco degli accessi non autorizzati)?			
Z5.3	è previsto l'utilizzo della VPN con MFA in caso di erogazione di assistenza da remoto?			
Z5.4	è effettuato il continuo patching applicativo di sicurezza relativo alla piattaforma per l'erogazione del supporto da remoto?			
Z5.5	è garantito il monitoraggio delle attività svolte dagli operatori con utenze privilegiate?			
Z5.6	le richieste di assistenza provengano da un soggetto identificato e preventivamente autorizzato dal Cliente?			
Z5.7	l'accesso agli ambienti di produzione da parte di Utenti che non operano in qualità di amministratori di sistema è consentito unicamente in presenza di comprovate esigenze di assistenza/manutenzione e mediante un processo autorizzativo ad hoc?			
Z5.8	gli operatori incaricati dell'assistenza utilizzano utenze individuali?			
Z5.9	gli accessi degli operatori incaricati dell'assistenza sono loggati?			
Z5.10	l'eventuale copia o trasferimento di archivi o base dati del Cliente per finalità di assistenza o manutenzione è preventivamente ed espressamente autorizzata dal Cliente?			
Z5.11	i DB/archivi del Cliente sono conservati solo per il tempo necessario all'esecuzione dell'attività di assistenza?			
Z5.12	i DB/archivi del Cliente sono immediatamente cancellati quando non più necessari per l'attività di assistenza?			
Z5.13	le copie dei DB/archivi del Cliente prelevati per finalità di assistenza sono trasferite tramite canali sicuri e protetti?			
Z5.14	le copie dei DB/archivi prelevate per finalità di assistenza sono salvate in ambienti con misure di sicurezza adeguate?			
Z5.15	i documenti stampati durante l'assistenza sono protetti contro accessi non autorizzati?			
Z5.16	i documenti stampati relativi all'assistenza sono distrutti al termine dell'attività di assistenza?			
Z5.17	i dati sono trasmessi utilizzando canali sicuri e protetti?			
Z5.18	le basi dati contenenti dati effettivi sono utilizzate in ambienti dedicati con misure di sicurezza adeguate?			
Z5.19	i profili di accesso agli ambienti sono configurati solo per il personale preposto dalla SWH?			
Z5.20	i dati sono conservati solo fino al completamento delle attività di verifica e accettazione da parte del Cliente?			
Z5.21	sono adottati processi e strumenti di assistenza che assicurano la tracciabilità degli interventi richiesti ed eseguiti			
Z6	Sono adottati software gestionali in cloud?			
Z6.1	In caso di risposta affermativa alla domanda Z6, è stato verificato che:			
Z6.2	gli accessi di amministrazione da parte della SWH sono riservati al personale con qualifica di amministratore di sistema?			
Z6.3	l'accesso amministrativo ai sistemi da parte del personale del Cliente avviene tramite autenticazione a più fattori (MFA)?			
Z6.4	In caso di utilizzo di servizi che prevedono una modalità di gestione amministrativa delle componenti infrastrutturali:			
Z6.5	le utenze consentono l'indivudazione dell'amministratore che esegue l'intervento?			
Z6.6	è attivato un processo di log management che identifichi log in, log out, log in failed?			
Z6.7	è prevista la conservazione dei log in un formato che garantisca l'integrità e la lettura nel tempo?			
Z6.8	il sistema di gestione e analisi dei log è utilizzato per monitorare le attività degli amministratori di sistema?			
Z6.9	l'accesso al sistema di gestione dei log è riservato al personale con ruolo di auditor?			
Z6.10	sono applicati protocolli crittografici standard di comunicazione sicuri e non obsoleti per l'accesso al sistema tramite Internet?			
Z6.11	è adottato un programma di gestione delle minacce e dei rischi per monitorare le vulnerabilità delle Piattaforme SaaS indicato da best practice internazionali?			
Z6.12	sono pianificate ed eseguite scansioni delle vulnerabilità interne ed esterne e test di penetrazione?			
Z6.13	è adottato un programma di gestione delle minacce e dei rischi per monitorare le vulnerabilità delle Piattaforme SaaS?			
Z6.14	le vulnerabilità identificate sono valutate per determinare i rischi associati e le azioni correttive sono stabilite in base alla priorità e gravità?			
Z6.15	sono adottati sistemi di firewall per filtrare e contenere il traffico, identificando eventuale traffico anomalo?			
Z6.16	l'ambiente di erogazione del servizio è protetto da un Intrusion Prevention System (IPS)?			

Z6.17	sono adottate misure di protezione da infezioni di software malevolo, di difesa da azioni non autorizzate, da applicazioni sospette e di protezione da tentativi di sottrazione di dati personali (es. mediante sistemi antivirus, antispamming, antiphishing, etc., mantenuti costantemente aggiornati)?			
Z6.18	sono adottati moduli Antivirus sul filesystem su tutti i server utilizzati per la fornitura dei servizi?			
Z6.19	sono adottate policy e procedure per l'identificazione, gli interventi, i rimedi e le segnalazioni di incidenti che determinano un rischio per l'integrità o riservatezza dei dati personali o altre violazioni della sicurezza?			
Z6.20	la piattaforma è sottoposta ad un processo di verifica delle patch relativamente alle componenti dell'impianto di erogazione?			
Z6.21	sono applicate adeguate misure di sicurezza fisica alla piattaforma hardware/software progettata (es. utilizzo di hosting providers/servizi di data center dotati di adeguati sistemi di prevenzione del rischio intrusione, incendio, allagamento, ecc.)?			
Z6.22	sono previste delle misure per la cancellazione dei dati di produzione al termine dell'erogazione del servizio secondo i termini contrattuali definiti con il Cliente?			
Z6.23	sono previsti dei requisiti del sub-fornitore che assume la gestione sistemistica dei server e dell'infrastruttura necessari allo svolgimento dei Servizi e sottoscrizione di un contratto che vincoli il medesimo sub-fornitore al rispetto degli obblighi concernenti le misure di sicurezza?			
Z6.24	il fornitore che gestisce il DC esterno è sottoposto ad audit periodici per la verifica del rispetto degli obblighi concernenti le misure di sicurezza?			
Z6.25	è effettuata l'erogazione periodica di corsi di formazione sulla sicurezza e protezione dei dati personali nei cofronti del personale coinvolto nelle attività di trattamento?			
Z6.26	sono adottate procedure di individuazione, contenimento e risoluzione di situazioni di rischio(e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post- instrusione?			
Z6.27	è effettuata la rivalutazione delle misure e procedure di sicurezza applicate?			
X	**REQUISITI SPECIFICI PER LA PROTEZIONE DELLE BANCHE DATI ("Linee Guida per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio", pubblicate dall'Agenzia per la Cybersicurezza Nazionale in data 26 Novembre 2024)**	**SI**	**NO**	**N/A**
X1	**Controllo accessi**			
X1.1	Le identità digitali degli utenti, dispositivi e processi autorizzati sono correttamente amministrate?			
X1.2	Le credenziali di accesso sono verificate regolarmente?			
X1.3	E' presente una procedura per la revoca delle credenziali di accesso non più necessarie?			
X1.4	Viene effettuato un audit di sicurezza periodico sulle credenziali di accesso?			
X1.5	Sono presenti misure di controllo per amministrare l'accesso fisico alle risorse?			
X1.6	Le aree sensibili sono dotate di sistemi di sicurezza fisica (es. badge, serrature elettroniche)?			
X1.7	Sono implementate misure di sicurezza per proteggere l'accesso remoto (es. VPN, autenticazione a due fattori)?			
X1.8	Viene monitorato l'accesso remoto per rilevare eventuali attività sospette?			
X1.9	I diritti di accesso alle risorse sono assegnati secondo il principio del privilegio minimo e della separazione delle funzioni?			
X1.10	L'integrità della rete è protetta tramite misure di segregazione e segmentazione?			
X1.11	Le modalità di autenticazione (es. autenticazione a fattore singolo o multiplo) per gli utenti, i dispositivi e altri asset sono commisurate al rischio della transazione (es. rischi legati alla sicurezza e privacy degli individui e altri rischi dell'organizzazione)?			
X1.12	La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati?			
X2	**Applicazione di principi e buone pratiche di sviluppo sicuro dei sistemi e delle applicazioni**			
X2.1	Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT che incorporano principi di sicurezza (es. principio di minima funzionalità)?			
X2.2	In caso di risposta affermativa alla domanda X.2.1:			
X2.3	le baseline incorporate includono principi di sicurezza come il principio di minima funzionalità?			
X2.4	le configurazioni dei sistemi sono regolarmente riviste e aggiornate per mantenere la sicurezza?			
X2.5	i backup sono eseguiti, amministrati e verificati periodicamente?			
X2.6	i dati e le informazioni memorizzati sono protetti?			
X2.7	esistono procedure per garantire che i dati di produzione non vengano utilizzati negli ambienti di sviluppo e test?			
X3	**Gestione del ciclo di vita dei sistemi e delle applicazioni**			
X3.1	Il processo di gestione del ciclo di vita dei sistemi include fasi di pianificazione, sviluppo, test, implementazione e manutenzione?			
X3.2	La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati?			
X3.3	La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati?			
X3.4	È implementato un processo per la gestione del ciclo di vita dei sistemi (System Development Life Cycle)?			
X3.5	Il trasferimento fisico, la rimozione e la distruzione dei dispositivi atti alla memorizzazione di dati sono gestiti attraverso un processo formale?			
X3.6	sono svolte scansioni per le identificazioni delle vulnerabilità?			
X4	**Gestione dei rischi e sicurezza della catena di approvvigionamento**			
X4.1	I processi di gestione del rischio inerenti la catena di approvvigionamento cyber sono identificati, ben definiti, validati, gestiti e approvati da attori interni all'organizzazione?			
X4.2	I fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber?			

X4.3	Sono indicate nei contratti con ulteriori fornitori gli obiettivi del programma di cybersecurity dell'organizzazione e del Piano di Gestione del Rischio della catena di approvvigionamento cyber?			
X5	**Monitoraggio e auditing**			
X5.1	i flussi di dati e comunicazioni inerenti l'organizzazione sono identificati?			
X5.3	esiste ed è attuata una policy per definire, implementare e revisionare i log dei sistemi?			
X5.4	le reti di comunicazione e controllo sono protette?			
X5.5	le informazioni relative agli eventi sono raccolte e correlate da sensori e sorgenti multiple?			
X5.6	è effettuato il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity?			
X5.7	Il codice malevolo viene rilevato?			
X5.8	è effettuato il monitoraggio per rilevare personale, connessioni, dispositivi o software non autorizzati?			
X5.9	ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability?			
X6	**Formazione del personale**			
X6.1	tutti gli utenti effettuano delle sessioni formative adeguate?			
X6.2	gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità?			

versione 1.2 aprile 2025

NOTA: Tale sezione deve essere compilata solo dai soggetti che rientrano nell' ambito di applicazione dell'articolo 1 , comma 1, della Legge 28 giugno 2024, n. 90

Y	**Linee Guida per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90**	SI	NO	N/A
Y1	Il Responsabile rientra tra i soggetti individuati dall'articolo 1 comma 1, della legge 28 giugno 2024, n. 90?			
Y2	In caso di risposta affermativa alla domanda Y1:			
Y2.1	i sistemi e gli apparati fisici sono censiti?			
Y2.2	esiste un elenco di quelli approvati da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90?			
Y2.3	l'accesso alla rete è consentito esclusivamente ai soli sistemi e apparati fisici approvati?			
Y2.4	sono censite le piattaforme e le applicazioni software in uso nell'organizzazione?			
Y2.5	esiste un elenco di quelle approvate da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024, n. 90?			
Y2.6	l'installazione è consentita esclusivamente alle piattaforme e applicazioni software approvate?			
Y2.7	sono identificati i flussi di dati inerenti all'organizzazione?			
Y2.8	tutti i flussi informativi tra i sistemi informativi e di rete del soggetto e l'esterno sono identificati?			
Y2.9	esiste un elenco di quelli approvati da attori interni alla struttura di cui all'articolo 8 della legge 28 giugno 2024,n. 90?			
Y2.10	le comunicazioni sono consentite unicamente per i flussi informativi approvati?			
Y2.11	sono definiti i ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)?			
Y2.12	è definita e resa nota alle articolazioni del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti?			
Y2.13	è istituita e resa nota alle articolazioni del soggetto la struttura di cui all'articolo 8, comma 1, della Legge 28 giugno 2024, n. 90?			
Y2.14	è nominato, nell'ambito della struttura di cui al punto precedente, il referente per la cybersicurezza di cui all'articolo 8,comma 2, della Legge 28 giugno 2024, n. 90, in possesso di specifiche e comprovate professionalità e competenze in materia di cybersicurezza?			
Y2.15	è identificata e resa nota una Policy di cybersecurity?			
Y2.16	In caso di risposta affermativa alla domanda Y2.15 indicare quali dei seguenti ambiti sono compresi nella policy di cybersecurity:			
Y2.16.1	governo			
Y2.16.2	gestione del rischio			
Y2.16.3	gestione degli asset			
Y2.16.4	gestione del rischio di cybersecurity della catena di approvvigionamento			
Y2.16.5	gestione delle vulnerabilità			
Y2.16.6	business continuity e disaster recovery			
Y2.16.7	gestione delle identità digitali e del controllo access			
Y2.16.8	sicurezza dei dati			
Y2.16.9	manutenzione e riparazione dei sistemi;			
Y2.16.10	protezione delle reti			
Y2.16.11	monitoraggio degli eventi di sicurezza			
Y2.16.12	risposta e ripristino agli incidenti			
Y2.16.13	formazione del personale.			
Y2.16.14	le politiche e i processi di cybersecurity vengono revisionati periodicamente e quando necessario?			
Y2.16.15	è presente un piano programmatico aggiornato per la sicurezza di dati, sistemi e infrastrutture in accordo alle politiche di cybersecurity?			
Y2.17	la governance ed i processi di risk management includono la gestione dei rischi legati alla cybersecurity?			
Y2.18	è presente un piano aggiornato per la gestione del rischio informatico?			
Y2.19	le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate?			
Y2.20	è presente un piano di gestione delle vulnerabilità?			
Y2.21	In caso di risposta affermativa alla domanda Y2.20:			
Y2.21.1	tale piano contiene almeno le modalità per l'identificazione delle vulnerabilità?			
Y2.21.2	Il piano viene aggiornato periodicamente?			
Y2.22	le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio?			
Y2.23	è presente un documento aggiornato di valutazione del rischio (risk assessment), sviluppato in accordo con il piano di gestione di rischio informatico?			
Y2.24	In caso di risposta affermativa alla domanda Y2.23, il documento comprende almeno:			
Y2.24.1	l'identificazione del rischio			
Y2.24.2	l'analisi del rischio			
Y2.24.3	la ponderazione del rischio			
Y2.25	la valutazione del rischio è effettuata considerando le minacce interne ed esterne, le vulnerabilità, le probabilità di accadimento e i conseguenti impatti?			
Y2.26	sono identificate e prioritizzate le risposte al rischio?			
Y2.27	esiste un documento aggiornato che descrive le scelte operate in merito al trattamento di ciascun rischio individuato e le relative priorità?			
Y2.28	esiste un documento aggiornato ed approvato, contenente la descrizione del rischio residuo successivo al trattamento di ciascun rischio individuato e le relative priorità, con il quale si accetta il rischio residuo?			
Y2.29	i fornitori e i partner terzi di sistemi informatici, componenti e servizi sono identificati, prioritizzati e valutati utilizzando un processo di valutazione del rischio inerente la catena di approvvigionamento cyber?			
Y2.30	salvo motivate e documentate ragioni di natura organizzativa o tecnica, le identità digitali sono individuali per gli utenti?			
Y2.31	le credenziali di accesso relative alle identità digitali sono robuste e aggiornate con una cadenza proporzionata ai privilegi dell'utenza?			
Y2.32	sono verificate periodicamente le identità digitali e le credenziali di accesso, aggiornandole/revocandole in caso di variazioni (es. trasferimento o cessazione di personale)?			
Y2.33	l'accesso remoto alle risorse è amministrato?			
Y2.34	i diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni?			
Y2.35	è presente un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi di gestione dei diritti di accesso e alle relative autorizzazioni?			
Y2.36	tutti gli utenti sono stati opportunamente informati e addestrati?			
Y2.37	è presente un documento aggiornato contenente l'elenco degli utenti che hanno ricevuto la formazione, i relativi contenuti,e la verifica dell'acquisizione di tali contenuti?			
Y2.38	è presente un documento aggiornato contenente l'elenco degli ADS che hanno ricevuto la formazione, i relativi contenuti e le modalità di verifica dell'acquisizione di tali contenuti?			
Y2.39	per proteggere i dati da memorizzare (in particolare sui dispositivi portatili e rimovibili) ove applicabile, sono utilizzati sistemi di cifratura dei dati e in particolare per i dispositivi portatili e quelli removibili?			
Y2.40	sono effettuati periodicamente, amministrati e verificati i backup dei dati?			
Y2.41	è assicurata la riservatezza delle informazioni contenute nei backup mediante adeguata protezione fisica dei supporti ovvero mediante cifratura?			
Y2.43	viene verificata periodicamente l'utilizzabilità dei backup effettuati, mediante test di ripristino?			
Y2.44	sono attivi ed amministrati piani di risposta (Incident Response e Business Continuity) in caso di incidente/disastro?			
Y2.45	sono attivi ed amministrati piani di recupero (Incident Recovery e Disaster Recovery)?			
Y2.46	è sviluppato e implementato un piano di gestione delle vulnerabilità?			
Y2.47	le vulnerabilità delle risorse dell'organizzazione sono prontamente risolte attraverso aggiornamenti di sicurezza o misure di mitigazione, ove disponibili, ovvero accentando il rischio in accordo al piano di gestione del rischio informatico?			
Y2.48	le vulnerabilità segnalate da ACN, vengono risolte, senza ritardo e comunque non oltre 15 gg. dalla segnalazione, adottando gli interventi indicati dall'Agenzia stessa?			
Y2.49	per le vulnerabilità segnalate da ACN che non possono essere risolte qualora sussistano motivate esigenze di natura tecnico-organizzativa che ne impedisca l'adozione, o comportino il differimento oltre il termine indicato degli interventi, è data tempestiva comunicazione all'Agenzia?			
Y2.50	La manutenzione e la riparazione delle risorse e dei sistemi è eseguita e registrata con strumenti controllati ed autorizzati?			
Y2.51	Le reti di comunicazione e controllo sono protette?			
Y2.52	Sono presenti e aggiornati i sistemi perimetrali anche a livello applicativo?			
Y2.53	In relazione alla protezione delle reti, è presente un documento aggiornato contenente almeno le procedure e gli strumenti tecnici impiegati per il rispetto delle politiche e nell'ambito dei processi di cybersecurity?			
Y2.54	Viene effettuato il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity?			
Y2.55	Sono presenti e aggiornati sistemi di rilevamento delle intrusioni (intrusion detection systems - IDS)?			
Y2.56	è monitorato il traffico in ingresso e uscita, le attività dei sistemi perimetrali, quali router e firewall, gli eventi amministrativi di rilievo, nonché gli accessi eseguiti o falliti alle risorse di rete e alle postazioni terminali al fine di rilevare gli eventi di cybersecurity?			
Y2.57	è presente un documento aggiornato contenente almeno le procedure, metodologie e tecnologie impiegate per il rispetto delle politiche e nell'ambito dei processi processi di cybersecurity?			
Y2.58	Il codice malevolo viene rilevato?			
Y2.59	Sono utilizzati strumenti di analisi e filtraggio sul flusso di traffico in ingresso (posta elettronica, download, dispositivi removibili, ecc.)?			
Y2.60	è presente un piano di risposta (response plan) aggiornato che viene eseguito durante o dopo un incidente?			
Y2.61	sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione?(es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)			
Y2.62	esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity			