ALLEGATO I - Checklist - Questionario per la verifica del regolamento (UE) 2016/679

	ALLEGATO I - Checklist - Questionario per la verifica del regolamento (UE) 2016/679	CIT	NO	BT/A
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?			
В	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?	51	210	1,012
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			
	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.			
В3	Il Registro viene regolarmente aggiornato?			
С	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
	Sono stati designati 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?			
	i soggetti autorizzati al trattamento sono vincolati ad un obbligo, legalmente assunto, di riservatezza?			
	Alcune attività vengono svolte in modalità di "lavoro agile"?			
	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:			
	Sono stati sottoscritti appositi atti di designazione individuale?			
	Sono state impartire adeguate istruzioni ai designati secondo i ruoli assegnati?			
	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?			
	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 <i>user id</i> 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 <i>user id</i> attribuite agli Amministratori che, per qualunque motivo, non necessitano più di accedere ai dati.			
E5	Le password associate alle <i>user id</i> assegnate agli Amministratori prevedono il rispetto delle seguenti regole?			
	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);			
	le password sono conservate in modo da garantirne disponibilità e riservatezza;			
E5.5	registrazione di tutte le immissioni errate di <i>password</i> ;			
E6	Gli account degli Amministratori sono bloccati dopo un numero massimo di tentativi falliti di login, ove tecnicamente possibile?			

F7   L'archiviazione di password ocodici PN, su qualsiasi supporto fisico avvesgo, è protenta da sistemi di cifratura?
privilegiate, alle quali devono corrispondere credenzial diverse?  By I profile dia excesso per le utenze di ADS rispettano il principio del need-to-know, ovvero che non siano attribuiti diritti otre a quelli realmente necessari per eseguire le artività di lavoro?  Lo di diritti otre a quelli realmente necessari per eseguire le artività di lavoro?  Lo diritti otre a quelli realmente necessari per eseguire le artività di lavoro?  Lo di antività e de quando sono aumentati i diritti di una utenza amministrativa giù attiva?  El 12 la conservazione dei regiori degli accessal logici (fog) degli Amministrativa e di sistemi?  El 12 la conservazione dei regiori degli accessal logici (fog) degli Amministrativa giù attiva?  El 13 conservazione dei regiori degli accessal logici e gamntin per ne periodo non inferiora a o mesti?  El 14 conservazione dei regiori degli accessal logici e gamntin per me periodo non inferiora a di sistemi?  Sono state adottate idonee misure finalizzate ad obbligare l'Amministratore ad accedere ai sistemi con una utenza normalica e solo successivamente eseguiri e istegici comandi come ADS?  Sono state commicati al momento della sottoscrizione dell'atto di designazione e con cadenza almeno annuale o ogni qualvotto se ne verifichi la necessità alla Regione Lazio gli esternii disnificativi dei soggetti nominiati Amministratori di Sistema?  El Sono state adottate idonee misure per consentire di mettree a disposizione del Titolare e del RPD della Regione Lazio e informazioni estativa a log delle operazioni per un periodo di 6 mesi, qualora necessario?  F PRIVACY BY DESIGNE BY DEFAULT  Prosonstate adottate lopolitiche ariendali di protezione dari fin dalla progettazione (privacy by design by default) affinchè le stesse possano adeguarsi ai mutamenti tecnologici e all'inorgere di nuovi ricchi?  P Sono state adottate la politiche ariendali di protezione dari fin dalla prosonali?  Sono state seguitate le valuazioni del rischipi per relascuita transmento?  F Sono state soditati di minutazioni del rischipi p
diriti oftre a quelli realmente necessari per eseguire le attività di lavoro?  I distensiva sono dotati di triumenti automatici fron derir che si attivano ad esempio quando viene aggiunta una utenza amministrativa già attiva?  El 11 Sono stati adottati sistenti di registrazione degli accessi logici (20) degli Amministratori a sistenti?  El 12 La conservazione dei registri degli accessi logici è garantita per un periodo non inferiore a 6 mesi?  El 2 La conservazione dei registri degli accessi logici è garantita per un periodo non inferiore a 6 mesi?  El 3 Regione sessa pracederà alla registrazione e conservazione del fog?  El 3 Sono state adottate idonee misure tinulizzare adollelare l'Amministratore ad accodera al sistemi con una utenza normale e solo successivamente eseguire i suntinizzatore adollelare l'Amministratore ad accodera al sistemi con una utenza normale e solo successivamente eseguire i singoli comandi come ADS?  Sono state adottate idonee misure tinulizzare adollelare l'Amministratore ad accodera al sistemi con una utenza normale e solo successivamente eseguire i suntinizatori adolle a regione l'accidentificativi dei soggetti nominati Amministratori di Sistema?  El 50 Sono state adottate idonee misure per consentire di mettere a disposizione del Titolare e del RPD della Regione Lazio e informazioni relativa ai fog delle operazioni per un periodo di 6 mesi, qualora necessario?  F P SI Sono state adottate idonee misure per consentire di mettere a disposizione del Titolare e del RPD della Regione Lazio e informazioni relativa ai fog delle operazioni per un periodo di 6 mesi, qualora necessario?  E stato adottato sistema di monitoraggio delle politiche aziendali di privacy by designe by default affinchè le stesse possono adequarsi ai mutamenti tecnologici e all'insorgere di muori rischi?  E stato adottato sistema di monitoraggio delle politiche aziendali di privacy by designe by default affinchè le stesse possono adequarsi ai mutamenti tecnologici e all'insorgere di muori rischi?  E sono state sortitut
Estato isono dotati di strumenti automatici tipo alerr che si attivano ad esempio quando viene aggiunta una utenza imanistratirativa dei quando sono aumentati diritti di una utenza amministrativa gii attiva?
E11] sono stati adottati sistemi di registrazione degli accessi logici (log) degli Amministratori ai sistemi?  E12] at conservazione dei registri degli accessi logici è gamantia per un periodo non inferiore a fonesi?  E13 no 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?  E15 Sono state adottate idone misure finalizare al obbligare l'Amministratore ad accedere ai sistemi con una utenza normale e solo successivamente eseguire i singoli comundi come ADS?  Sono state adottate idone misure finalizare al obbligare l'Amministratori e accedera al sistemi con una utenza normale e solo successivamente eseguire i singoli comundi come ADS?  Sono state adottate i onomento della sottostrazione dell' rodi dissignazione 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 i olone misure per consentire di mettere a disposizione del Tinolare e del RPD della Regione Lazio gli informazioni relativi au log delle operazioni per un periodo di 6 mesi, qualora necessario?  F PRIVACY BY DESIGNE BY DEPAULT  SI NO N/  E1 Sono state adottate i politiche aziendali di privacy by designi e by default affinchè le stesse prossumo adeguarsi ai minamenti cenologici e all'insoquere di monori rischi?  E3 Sono state eseguiste le valutazioni del rischio per ciascun trattamento?  E4 Sono state struttura le operazioni in modo da minimizzare il trattamento dei dati personali?  E5 Sono state definiti i ruoli e le responsabilità relativa il trattamento dei dati personali?  Sono state desiniti i ruoli e le responsabilità relativa il trattamento dei dati personali?  Sono state desiniti i ruoli e le responsabilità relativa il trattamento dei dati personali?  G1 In accessi di cui al alla d
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 del log ?  El 4 Sono state adottate idonce misure finalizzate ad obbligare l'Amministratore ad accedere ai sistemi con una utenza normale e solo successivamente eseguire i singoli comand come ADS?  Sono stati comunicati al momento della sottosserzione dell'alto di designazione e con cadenza almeno annuale o ogni gualvolta se ne verifichi la necessità alla Regione Lazio gli estremi identificativi dei soggetti nominati Amministratori di Sistema?  El 5 Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?  El 7 FI Sono state adottate lodonee misure per consentrie di mettere a disposizione del Triotare e del RPD della Regione Lazio gli estremi identificativi dei soggetti nominati Amministratori di Sistema?  FI Sono state adottate lodonee misure per consentrie di mettere a disposizione del Triotare e del RPD della Regione Lazio gli cittoria del richia della di privace proposano adeguarsi ai mutamenti tecnologici e all'insorgere di nuori rischi?  FI Sono state adottate lottati di protezione dati fin dalla progettazione (privace) by design ?  FI Sono state eseguiste le valutazioni del rischio per ciascun trattamento?  FI Sono state eseguiste le valutazioni del rischio per ciascun trattamento?  FI Sono state est utrutturate le operazioni in modo da minimizzare il trattamento dei dati personali?  FI Sono state dottate tutte le misure necessarie per perseguire la massima trasparenza dei trattamenti di dati personali rendendo accessibile agli interessati idonea documentazione?  GI Sono state dottate idonamada GI agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali?  Sono state messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio?  GI I pseudonimizzazione e/o la cifiratura dei dati personali?  So
Regione stessa procederà alla registrazione e conservazione dei log?  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?  Sono stati comunicati al montione della sottoscrizione dell'atto di designazione e con cadenza almeno annuale o ogni procedere alla della sottoscrizione dell'atto di designazione con cadenza almeno annuale o ogni sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?  Elio Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?  Elio Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?  F PRIVACY BY DESIGNE EW DEFAULT  Fi Sono state adottate i longe 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 DESIGNE EW DEFAULT  Fi Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (privacy by design p)?  F Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (privacy by design p)?  F Sono state assentiate le valutazioni del rischio per ciascun trattamento?  F Sono state assunturate le operazioni in moto da minimizzare il trattamento dei dati personali?  F Sono state assunturate le operazioni in moto da minimizzare il trattamento dei dati personali?  G MISURE DI SICUREZZA  SI NO N/  SI Sono state destita in una di protezione accumentazione?  G MISURE DI SICUREZZA  SI NO N/  G Il oso stati definiti i note le responsabilità relativi al trattamento dei dati personali?  G Il oso state messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio?  G Il neso di risposta affermativa alla domanda G3, le misure adottate comprendono:  G Il neso di risposta affermativa alla domanda G7:  G Sono state
Sono state adotate idonee misure frantizzate ad obbligare l'Amministratore ad accedere ai sistemi con una utenza normale e solo successivamente eseguire i singoli comandi come ADS?  Sono stati comministatori di Sistema?  E16 Sono state comministatori di Sistema?  E16 Sono state adottate idonee misure per consentire di mettere a disposizione del Titolare e del RPD della Regione Lazio gli estremi identificativi dei soggetti nominati Amministratori di Sistema?  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 DESIGNE EN DEFAULT  F1 Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (privacy by design ?)  F2 Sisto adottato sistema di monitoraggio delle politiche aziendali di privacy by design e by default affinche le stesse possibile associatione del rischio per ciasceni trattamento?  F3 Sono state strutturate le operazioni in modo da minimizzare il trattamento dei dati personali?  F3 Sono state adottate tutturale le operazioni in modo da minimizzare il trattamento dei dati personali?  F3 Sono state dottate tutturale le operazioni in modo da minimizzare il trattamento dei dati personali?  F3 Sono state dottate tutturale le operazioni in modo da minimizzare il trattamento dei dati personali?  F4 Sono state dottate tutturale le operazioni in modo da minimizzare il trattamento dei dati personali?  F5 Sono state dottate tutturale le operazioni in modo da minimizzare il trattamento dei dati personali?  F6 MISURE DI SICUREZZA  F8 SONO State messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio?  F8 Sono state adottate idonea documentazione dei dati personali?  F8 Sono state ensese in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio?  F8 Sono state predisposte misure evilutare regolarmente l'efficacia del
Sono state comunicati al momento della sottoscrizione dell'atto di designazione e con cadenza almeno annuale o ogni ell' qualvolta se ne verifichi la necessità alla Regione Lazio gli estremi identificativi dei soggetti mominati Amministratori di Sistema?   Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?   Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?   Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS?   Sono state adottate ichone misure per consentire di metrere a disposizione del Titolare e del RPD della Regione Lazio dei informazioni relative ai log elde loperazioni per un periodo di 6 mesi, qualora necessario?   Si No N/2   Sono state adottate istendi di protezione dati fin dalla progettazione (privacy by design p)?   Si Sono state adottate istendi di monitoraggio delle politiche aziendali di privacy by design e by default affinchè le stesse possano adeguarsi ai mutamenti tecnologici e all'insorgere di muovi rischi?   Sono state sutriturate le operazioni in modo da minimizzare il trattamento dei dati personali?   Sono state adottate lutte le misure necessarie per perseguire la massima trasparenza dei trattamenti di dati personali rendendo accessibile agli interessati idone adocumentazione?   Si No N/2   Sono state della di presonali in le le responsabilità relativi al trattamento dei dati personali?   Sono state della di personali in della domanda G1 agiscono secondo procedure interne definite per la gestione degli adempimenti mila procedio dei dati personali?   Sono state messe in atto misure tecniche e organizzative idone a garantire un livello di sicurezza adeguato al rischio?   Sono state messe in atto misure tecniche e organizzative idone a garantire un livello di sicurezza adeguato al rischio?   Sono state messe ano atto misure tecniche e organizzative idone a garantire al capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati person
E15 qualvolta se ne verifichi la necessità alla Regione Lazio gli estremi identificativi dei soggetti nominati Amministratori di Sistema?  E16 Sono state sesguite, con cadenza almeno annuale, le attività di verifica dell' operato degli ADS?  E17 Sono state sesguite, con cadenza almeno annuale, le attività di verifica dell' operato degli ADS?  E18 Sono state sesguite, con cadenza almeno annuale, le attività di verifica dell' operatori dell' all' all' all' all' all' all' all'
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  Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (privacy by design ?)?  E 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 dei rischio per ciascun trattamento?  F4 Sono state estrutturate 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  S1 NO N/a  G1 Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?  G2 I soggetti di cui al 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. In caso di risposta affermativa alla domanda G3, le misure adottate comprendono:  G4. misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?  misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?  G5 Sono state perdisposte misure tecniche che consentono l'accesso ai dati personali unicamente ai soggetti autorizzati?  G6 Sono state
F PRIVACY BY DESIGN E BY DEFAULT FI Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (privacy by design?)  E stato adottato sistema di monitoraggio delle politiche aziendali di privacy by design e by default affinchè le stesse possona odeguarsi ai mutamenti tenologici e all'insorgere di nuovi rischi? F3 Sono state eseguiste le valutazioni del rischio per ciascun trattamento? F4 Sono state eseguiste le valutazioni del rischio per ciascun trattamento? F5 Sono state ostrutturate le operazioni in modo da minimizzare il trattamento dei dati personali? F5 Sono state adottate tute 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/ G1 Sono stati definiti i notoli e le responsabilità relativi al trattamento dei dati personali? G2 suggetti di cui al 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 capacità di ripristinare tempestivamente 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 adottate almeno le misure minime di sicurezza id dati personali unicamente ai soggetti autorizzati? G6 Sono state adottate almeno le misure eminime di sicurezza id dati personali unicamente ai soggetti autorizzati? G7 È stata predipo
F PRIVACY BY DESIGN EN DEFAULT  Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (privacy by design)?  E 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 eseguiste le valutazioni del rischio per ciascun trattamento?  F4 Sono state eseguiste le valutazioni del rischio per ciascun trattamento?  Sono state eseguiste le valutazioni del rischio per ciascun trattamento?  F5 Sono state eseguiste le valutazioni del rischio per ciascun trattamento?  G MISURE DI SICUREZIA  G1 Sono state dottate tutte le misure necessarie per perseguire la massima trasparenza dei trattamenti di dati personali rendendo accessibile agli interessati i donea documentazione?  G MISURE DI SICUREZIA  G1 Sono state diffiniti i ruoli e le responsabilità relativi al trattamento dei dati personali?  G2 I soggetti di cui al 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?  G4.4 garantire donee a garantire la riservatezza, l'integrità, la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?  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 le l'integrata dei dati personali unicamente ai soggetti autorizzati?  G6 Sono state adottate almeno le misure minime di sicurezza lel Titolare?  G7 E stata prediposta idonea do
FI Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (privacy by design)?  E stato adottato sistema di monitoraggio delle politiche aziendali di privacy by design e by default affinchè le stesse possona odeguarsi ai mutamenti tecnologici e all'insorgere di nuovi rischi?  F3 Sono state eseguiste le valutazioni del rischio per ciascun trattamento?  F4 Sono state estrutturate 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  G1 Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?  G2 I soggetti di cui al 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?  G4.1 la pseudonimizzazione co 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 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:  G8.2 la documentazione è disponibile e producibile a ricchiesta del Titolare?  G10 È prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Ital
F3 Sono state seguiste le valutazioni del rischio per ciascun trattamento?  F3 Sono state seguiste 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 SUCINEZZA  SI NO N/2  G1 Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?  G2 Sono stati definiti i ruoli e le responsabilità relativi al trattamento 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:  G4-11 la pseudonimizzazione e/o la cifratura dei dati personali?  misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?  G4-2 misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?  G4-3 misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?  G5 Sono state predipsoste 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?  G8.2 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
F4 Sono state strutturate le operazioni in modo da minimizzare il trattamento dei dati personali?  Sono state adottate tutte le misure necessarie per perseguire la massima trasparenza dei trattamenti di dati personali redendo accessibile agli interessati idonea documentazione?  G MISURE DI SICUREZZA  SI NO N/  GI Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?  Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?  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?  misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?  G4-3.  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 predisposte misure tecniche che consentono l'accesso ai dati personali unicamente ai soggetti autorizzati?  G7 E stata prediposta idonea documentazione tecnica relativa alle misure di sicurezza in atto?  G8 In caso di risposta affermativa alla domanda G7:  G8. Ia documentazione de disponibile e producibile a richiesta del Titolare?  G9 E stato adottato un approccio alla sicurezza deil dati basato sul rischio?  G10 E presente un impianto antintrusione?  G11 Sono presenti procedure di controllo per l'accesso dei visitatori?  G11 Sono presenti procedure di controllo per l'accesso dei visitatori?  G11 Sono presenti procedure di controllo per l'accesso dei visitatori?  G12 Prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?  G13 processi di autenticazione
Sono state adottate tutte le misure necessarie per perseguire la massima trasparenza dei trattamenti di dati personali rendendo accessibile agli interessati idonea documentazione?   Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?   I soggetti di cui al alla domanda G1 agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali?   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?   misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?   misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?   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 E stata prediposta idonea documentazione tecnica relativa alle misure di sicurezza in atto?   G8 In caso di risposta affermativa alla domanda G7:   G8.2   la documentazione è disponibile e producibile a richiesta del Titolare?   G9 E stato adottato un approccio alla sicurezza dei dati basato sul rischio?   G10 E presente un impianto antitrusione?   G11 Sono presenti procedure di controllo per l'accesso dei visitatori?   G11 Sono presenti procedure di controllo per l'accesso dei visitatori?   E prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni cu
G MISURE DI SICUREZZA SI NO N/A  GI Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?  GI Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?  GI soggetti di cui al alla domanda GI agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali?  GS sono state messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al riscichio?  G4 In caso di risposta affermativa alla domanda G3, le misure adottate comprendono:  G4.1 la pseudonimizzazione e/o la cifratura dei dati personali?  misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?  G4.2 misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?  G5.3 misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?  G5.4 procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento?  G5.5 Sono state adottate almeno le misure tecniche che consentono l'accesso ai dati personali unicamente ai soggetti autorizzati?  G6.6 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?  G7.6 E stata prediposta idonea documentazione tecnica relativa alle misure di sicurezza in atto?  G8.2 la documentazione è disponibile e producibile a richiesta del Titolare?  G9.6 E stato adottato un approccio alla sicurezza dei dati basato sul rischio?  G10 E presente un impianto antintrusione?  G10 E presente un impianto antintrusione?  G10 E presente un impianto antintrusione?  G10 E prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, ass
GI Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali?  I soggetti di cui al alla domanda GI agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali?  Sono state messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio?  Gal In caso di risposta affermativa alla domanda G3, le misure adottate comprendono:  G4.1 la pseudonimizzazione e/o la cifratura dei dati personali?  misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?  misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico?  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:  G8.1 la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto?  G1.2 al documentazione è disponibile e producibile a richiesta del Titolare?  G1.3 bi adocumentazione è disponibile e producibile a richiesta del Titolare?  G1.4 bi adocumentazione è disponibile e producibile a richiesta del Titolare?  G1.5 prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?  G1.5 prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?
I soggetti di cui al alla domanda G1 agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali?   Sono state messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio?   G4
Sulla protezione dei dati personali?  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?  misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?  G4.2 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 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 E stata prediposta idonea documentazione tecnica relativa alle misure di sicurezza in atto?  G8 In caso di risposta affermativa alla domanda G7:  G8.1 la documentazione è disponibile e producibile a richiesta del Titolare?  G9 E stato adottato un approccio alla sicurezza dei dati basato sul rischio?  G10 E presente un impianto antintrusione?  G11 Sono presenti procedure di controllo per l'accesso dei visitatori?  E prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni eco!?  G10 i 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
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?  G8.1 la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto?  G8.2 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?  E prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?  G10 i 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
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:  G8.1 la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto?  G8.2 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?  E prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?  G1i 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
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?  G8.1 la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto?  G8.2 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)?  G1 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
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:  G8.1 la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto?  G8.2 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?  E prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?  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
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:  G8.1 la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto?  G8.2 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?  E prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?  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
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?  È prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?  G13 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
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)?  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
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)?  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
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)?  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
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)?  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
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)?  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
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)?  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
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)?  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
G12 È prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)?  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
Gli operatori autorizzati possono accedere ai dati trattati con strumenti informatici soltanto dopo almeno uno o due Gl3 processi di autenticazione (ad esempio il primo accesso al sistema operativo e il secondo accesso all'applicativo
G13 processi di autenticazione (ad esempio il primo accesso al sistema operativo e il secondo accesso all'applicativo
G14 Gli operatori autorizzati utilizzano credenziali di accesso individuali?
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 incaricati l'utilizzo di risorse informatiche (es.
È presente une presedure interne nel esse sie permesse si seggetti inceriagti l'utilizza di ricerse informatiche (es
G17 È presente una procedura interna, nel caso sia permesso ai soggetti incaricati l'utilizzo di risorse informatiche (es. PC, Tablet, smartphone) di proprietà di terzi?

G19.2 sono conservati i dati in <i>tenant</i> 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 <i>Disaster Recovery</i> ?  G19.8 è effettuata con cadenza temporale programmata <i>penetration test</i> sul sistema di elaborazione dei dati?  G19.9 è presente un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di e conservazione dei dati?  G19.10 è presente un impianto antintrusione?  G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?	laborazione e			
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 e conservazione dei dati?  G19.10 è presente un impianto antintrusione?  G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?	laborazione e			
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 <i>Disaster Recovery</i> ?  G19.8 è effettuata con cadenza temporale programmata <i>penetration test</i> sul sistema di elaborazione dei dati?  G19.9 è presente un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di e conservazione dei dati?  G19.10 è presente un impianto antintrusione?  G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?	laborazione e		į	
G19.6 è effettuato con cadenza temporale programmata un test sul Piano di Continuità Operativa?  G19.7 è presente un Piano di <i>Disaster Recovery</i> ?  G19.8 è effettuata con cadenza temporale programmata <i>penetration test</i> sul sistema di elaborazione dei dati?  G19.9 è presente un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di el conservazione dei dati?  G19.10 è presente un impianto antintrusione?  G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?	laborazione e			
G19.7 è presente un Piano di <i>Disaster Recovery</i> ?  G19.8 è effettuata con cadenza temporale programmata <i>penetration test</i> sul sistema di elaborazione dei dati?  G19.9 è presente un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di el conservazione dei dati?  G19.10 è presente un impianto antintrusione?  G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?	laborazione e			
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 el conservazione dei dati?  G19.10 è presente un impianto antintrusione?  G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?	laborazione e			
G19.9 è presente un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di el conservazione dei dati?  G19.10 è presente un impianto antintrusione?  G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?	laborazione e			
G19.9 è presente un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di el conservazione dei dati?  G19.10 è presente un impianto antintrusione?  G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?	laborazione e			
G19.10 è presente un impianto antintrusione? G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?				
G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?				
G19.11 sono presenti delle procedure per l'acceso controllato dei visitatori?				
			$\neg$	
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?				
G19.15 solio stati adoitati i sistemi di Crittografia per proteggere i dati ili transito:		-	-	
		$\longrightarrow$	-	
G19.17 è presente sistema SIEM?		$\longrightarrow$	$\longrightarrow$	
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 <i>firewall</i> , <i>intrusion detenction sistem</i> ecc.?		$\longrightarrow$	$\longrightarrow$	
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)?		<b></b> ↓		
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 s	senarati?			
37.22 sono utilizzati ambienti di svituppo sottware, test, conaudo e di produzione risicamente e logicamente s	вераган:			
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?			$\neg$	
G21.6 effettui con cadenza temporale programmata test sul Piano di Continuità Operativa?				
G21.7 disponga di un Piano di Disaster Recovery?			$\overline{}$	
G21.8 effettui con cadenza temporale programmata penetration test sul sistema di elaborazione dei dati?				
T	lahorogiana	$\longrightarrow$		
G21.9 sia dotato di un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di e			l	
GZ1.7 concernations dei deti?	iaborazione e			
conservazione dei dati?	iadorazione e			
conservazione dei dati?  G21.10 sia dotato di impianto antintrusione?	laborazione e			
conservazione dei dati?  G21.10 sia dotato di impianto antintrusione?  G21.11 sia dotato di procedure per l'acceso controllato dei visitatori?	iaborazione 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?	laborazione 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)?	laborazione 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?	laborazione 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?	iaborazione 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?	naborazione 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?	iaborazione 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?	iaborazione 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?	aborazione 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.?				
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.?				
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				
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 compatibilità con sistemi legacy)?	i tecniche o di			
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 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	i tecniche o di	SI	NO	N/A
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 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	i tecniche o di	SI	NO	N/A
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.?  non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?	i tecniche o di	SI	NO	N/A
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 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  H2 In caso di risposta affermativa alla domanda H1:	i tecniche o di	SI	NO	N/A
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 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  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?	i tecniche o di	SI	NO	N/A
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.? non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni 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 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?	i tecniche o di	SI	NO	N/A
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.?  non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni compatibilità con sistemi legacy)?  G21.20 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  H2.1 e 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 credenziali di accesso aile applicazioni?	i tecniche o di	SI	NO	N/A
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.?  non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  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?	i tecniche o di	SI	NO	N/A
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 SOC?  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.?  non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni compatibilità con sistemi legacy)?  G21.20 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  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?  prevede regole per la gestione degli accessi ad Internet?	i tecniche o di	SI	NO	N/A
conservazione dei dati?  G21.10 sia dotato di impianto antintrusione?  G21.11 sia dotato di impianto antintrusione?  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.?  non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  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 credenziali di accesso alle applicazioni?  H2.4 prevede regole per la gestione degli accessi a Social media (es: Facebook, You Tube, Twitter ecc)?  H2.5 prevede regole per la gestione e l'utilizzo della posta elettronica?	i tecniche o di	SI	NO	N/A
conservazione dei dati?  G21.10 sia dotato di impianto antintrusione?  G21.11 sia dotato di impianto antintrusione?  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 adotato 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 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  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 dei diritti di accesso ai dati?	i tecniche o di	SI	NO	N/A
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 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  H2.1 e 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 as ascial media (es: Facebook, You Tube, Twitter ecc)?  H2.6 prevede regole per la gestione dei diritti di accesso ai dati?  Provede regole per la gestione delli incidenti informatici?	i tecniche o di	SI	NO	N/A
conservazione dei dati?  G21.10 sia dotato di impianto antintrusione?  G21.11 sia dotato di impianto antintrusione?  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 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 PROCEDURE DI GESTIONE DEL SISTEMA INFORMATIVO AZIENDALE  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  H2.1 e 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 a social media (es: Facebook, You Tube, Twitter ecc)?  H2.5 prevede regole per la gestione dei diritti di accesso ai dati?  H2.6 prevede regole per la gestione dei diritti di accesso ai dati?  H2.7 prevede regole per la gestione dei diritti di accesso ai dati?  H2.8 prevede regole per la gestione dei diritti di accesso ai dati?  H2.9 prevede regole per la gestione dei diritti di accesso ai dati?  H2.9 prevede regole per la gestione dei diritti di accesso ai dati?	i tecniche o di	SI	NO	N/A
conservazione dei dati?  G21.10 sia dotato di impianto antintrusione?  G21.11 sia dotato di impianto antintrusione?  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 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  H2.1 prevede regole per la gestione delle credenziali di accesso ai database?  H2.2 prevede regole per la gestione degli accessi ad Internet?  H2.3 prevede regole per la gestione degli accessi a social media (es: Facebook , You Tube, Twitter ecc)?  H2.4 prevede regole per la gestione degli incidenti informatici?  H2.5 prevede regole per la gestione degli incidenti informatici?  H2.7 prevede regole per la gestione dei diritti di accesso ai data?  H2.8 prevede regole per la gestione degli incidenti informatici?  H2.9 prevede regole per la gestione dei diritti di accesso ai dati?  Prevede regole per la gestione dei diritti di accesso ai dati?  Prevede regole per la gestione dei diritti di accesso ai dati?  Prevede regole per la gestione dei diritti di accesso ai dati?  Prevede regole per la gestione dei diritti di accesso ai dati?  Prevede regole per	i tecniche o di	SI	NO	N/A
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 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  H1 Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale?  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 degli accessi a Internet?  H2.5 prevede regole per la gestione degli accessi al Internet?  H2.6 prevede regole per la gestione degli accessi a social media (es: Facebook, You Tube, Twitter ecc)?  H2.7 prevede regole per la gestione dei diritti di accesso ai dati?  H2.9 prevede regole per la gestione dei diritti di accesso ai dati?  H2.9 prevede regole per la gestione dei diritti di accesso ai dati?  H2.9 prevede regole per la gestione dei diritti di accesso ai dati?  H2.9 prevede regole per la gestione dei diritti di accesso ai dati?	i tecniche o di	SI	NO	N/A

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?			
	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)?			
	Sono state predisposte misure organizzative idonee a garantire la tempestiva informazione al Titolare ed al RPD			
I2	della Regione Lazio, (entro 24 ore dall'avvenuta conoscenza dell'evento), di ogni violazione di dati personali (data			
	breach)?			
	Sono state adottate misure organizzative idonee a garantire che l'informazione sulla violazione dei dati personali			
13	(data breach), sia corredata da tutta la documentazione utile per permettere al Titolare la tempestiva valutazione			
13	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?			
	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
	Sono state adottate misure tecniche ed organizzative idonee a garantire adeguata assistenza al Titolare nello			
L1	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?			
M2.2	È stato informato il Titolare del trattamento di eventuali modifiche riguardanti l'aggiunta di altri sub-responsabili o			
IVIZ.Z	la sostituzione sub-responsabili già nominati?			
	La nomina del cub responsabile à automute mediente un contratte e un eltre ette giunidice e norme del diritte			
M2 2	La nomina del sub-responsabile è avvenuta mediante un contratto o un altro atto giuridico a norma del diritto			
1012.3	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?			
	contratto (o in auto atto giuridico) da il Titolare dei dattamento e il Responsabile dei dattamento:			
	Nel contratto (o altro atto giuridico) di nomina è stato previsto che il sub-responsabile fornisca sufficienti garanzie			
M2.4	per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del			
	RGPD?			
M2.5	Il sub-responsabile nominato detiene un registro con le medesime caratteristiche formali ed i medesimi contenuti			
1412.5	sopra indicati relativamente ai trattamenti di competenza?			
M2.6	Nel contratto/altro atto giuridico sono state fornite adeguate istruzioni al sub-responsabile?			
M3	Sono effettuate periodiche verifiche sull'adeguatezza delle misure tecniche e organizzative adottate dal sub-			
1.10	responsabile?			
M4	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
N/1	Sono state adottate misure tecniche ed organizzative idonee a garantire la cancellazione o la restituzione di tutti i dati			
N1	personali nei termini stabiliti per la prestazione dei servizi o, comunque, a richiesta del Titolare?			
N/2	È			
	È presente una procedura operativa per la dismissione dei supporti dei dati?			
IN3	Sono presenti i dispositivi per la distruzione dei documenti cartacei?  TRASFERIMENTO DI DATI PERSONALI VERSO UN PAESE TERZO O UN'ORGANIZZAZIONE			
O	INTERNAZIONALE	SI	NO	N/A
	Sono effettuati trasferimenti di dati personali verso Paesi terzi o organizzazioni al di fuori dello Spazio Economico			
O1	Europeo?			
Ω2	In caso di risposta affermativa alla domanda O1:			
	è stata ottenuta l'autorizzazione scritta da parte del Titolare?			
	sono state adottate idonee misure per il rispetto del Capo V (artt. 44 - 50) del RGPD?			
P	CODICI DI CONDOTTA E CERTIFICAZIONI	SI	NO	N/A
	è prevista l'adesione a un codice di condotta ai sensi dell'art. 40 del RGPD?	51	110	1 1/11
	Si è in possesso della certificazione ISO 9001?			
	Si è in possesso della certificazione ISO 27001?			
	è presente altra certificazione rilasciata da organismi di certificazione di cui all'articolo 43 del RGPD o dall'autorità			
P4	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
	Sono state adottate procedure atte a consentire l'esercizio dei diritti degli interessati?	)I	110	. 1/ /L
	In caso di risposta affermativa alla domanda Q1 sono previste procedure per:			
	la limitazione del trattamento?			
	la portabilità dei dati?			
	la cancellazione dei dati su richiesta dell'interessato?			
	la cancellazione dei dati al termine del periodo previsto?			
	l'estrazione dei dati su richiesta dell'interessato?			
· • • • • • • • • • • • • • • • • • • •	restructione del uati su ficinesta den interessato:			

02.6	la mattifica dei deti?	ı		
	la rettifica dei dati?			
Q2.7	la gestione dell'opposizione al trattamento?  Sono state adottate misure tecniche ed organizzative idonee ad assistere il Titolare nel dare seguito alle richieste per			
Q3	l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD?			
04	Sono state ricevute istanze degli interessati in esercizio ai diritti di cui agli articoli da 15 a 22 del RGPD?			
	In caso di risposta affermativa alla domanda Q4:			
Q3	è stata effettuata tempestiva comunicazione scritta al Titolare e al RPD della Regione Lazio, allegando copia della			
Q5.1	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
	È utilizzato un sistema di autenticazione federato (es. LDAP, Spid, ecc.)?	, DI	110	1 1/11
R2	·			
	Sono state adottate le misure tecniche previste nelle <i>Linee Guida Funzioni Crittografiche – Conservazione delle</i>			
200	Password approvate con provvedimento del Garante registro n. 594 del 7 dicembre 2023 al fine di proteggere in			
R2.1	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:			
	Sono state adottate totalmente le misure tecniche previste?			
	Sono state adottate parzialmente le misure tecniche previste?			
	Sono state fornite idonee istruzioni agli Amministratori di sistema?			
	Sono state fornite idonee istruzioni ai sub-responsabili ove nominati?			
	In caso di affidamenti di puovi sarvizi à stato pravisto pravisto l'insarimento di apposita clausola nai capitalati			
R3.5	tecnici di gara?			
R4	In caso di risposta negativa alla domanda R2.1:			
	Sono state comunicate la circostanze al Titolare del trattamento?			
	È possibile comprovare che le misure tecniche adottate garantiscano comunque un livello di sicurezza adeguato al			
R4.2	rischio per i diritti e le libertà delle persone fisiche?			
	nel determinare il periodo di conservazione delle password, è previsto l'adeguato alle indicazioni sui criteri da			
R4.3	utilizzare fornite dal Garante nel provvedimento registro n. 594 del 7 dicembre 2023?			
	le password sono tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per			
R4.4	verificare l'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online?			
212	le password sono tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per			
R4.5	garantirne la sicurezza dei sistemi informatici o servizi online?			
D.4.6	le password sono tempestivamente cancellate, anche in modo automatico in caso di cessazione dei sistemi			
R4.6	informatici o servizi online?			
D4.7	le password sono tempestivamente cancellate, anche in modo automaticoin caso di disattivazione delle relative			
R4.7	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			
31	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?			
	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?			
	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
<b>T</b> 1	Sono effettuate forniture di servizi di sviluppo applicativo?			
T2				
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?			
Т3	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
	Sono effettuate forniture di oggetti connessi in rete?			
	In caso di risposta affermativa alla domanda T1:			
	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?		
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?		