

| CHECK LIST - ISTRUZIONI PER LA COMPILAZIONE | |
|---|---|
| ANAGRAFICA | L'anagrafica va compilata in ogni sua parte |
| ANAGRAFICA - PERIODO DI RIFERIMENTO | E' il periodo a cui si riferiscono le risposte del questionario. I campi "dal" "al" vanno valorizzati con le rispettive date nel formato gg/mm/aaaa. |
| QUESTIONARIO- COLONNE SI - NO - N/A | Tutte le domande del questionario prevedono una risposta attraverso la valorizzazione dei campi "SI", "NO" o "N/A" con una "X" nella colonna di interesse. Non devono essere lasciate domande senza risposta. |
| QUESTIONARIO - UTILIZZO DELLA COLONNA N/A | Il campo N/A deve essere valorizzato esclusivamente in caso di fattispecie non applicabile. |
| QUESTIONARIO- SEZIONE M - RICORSO AD ALTRO RESPONSABILE (di seguito SUB-RESPONSABILE) | La sezione deve essere compilata unicamente qualora il Responsabile ricorra ad uno o più altri responsabili (sub-responsabili) e deve essere ripetuta con riferimento ad ogni altro responsabile nominato. |

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

VERSIONE 1.0

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

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

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

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

| | | | | |
|----------|---|-----------|-----------|------------|
| E5.5 | registrazione di tutte le immissioni errate di <i>password</i> ; | | | |
| E6 | Gli <i>account</i> degli Amministratori sono bloccati dopo un numero massimo di tentativi falliti di <i>login</i> , ove tecnicamente possibile? | | | |
| E7 | L'archiviazione di <i>password</i> o codici PIN, su qualsiasi supporto fisico avvenga, è protetta da sistemi di cifratura? | | | |
| E8 | È assicurata la completa distinzione, in capo al medesimo utente, tra utenze privilegiate (amministratore) e non privilegiate, alle quali devono corrispondere credenziali diverse? | | | |
| E9 | I profili di accesso per le utenze di ADS rispettano il principio del <i>need-to-know</i> , ovvero che non siano attribuiti diritti oltre a quelli realmente necessari per eseguire le attività di lavoro? | | | |
| E10 | I sistemi sono dotati di strumenti automatici tipo <i>alert</i> che si attivano ad esempio quando viene aggiunta una utenza amministrativa e/o quando sono aumentati i diritti di una utenza amministrativa già attiva? | | | |
| E11 | Sono stati adottati sistemi di registrazione degli accessi logici (<i>log</i>) degli Amministratori ai sistemi? | | | |
| E12 | La conservazione dei registri degli accessi logici è garantita per un periodo non inferiore a 6 mesi? | | | |
| E13 | In caso di utilizzo di sistemi messi a disposizione dalla Regione, è stato comunicato agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei <i>log</i> ? | | | |
| E14 | Sono state adottate idonee misure finalizzate ad obbligare l'Amministratore ad accedere ai sistemi con una utenza normale e solo successivamente eseguire i singoli comandi come ADS? | | | |
| E15 | Sono stati comunicati al momento della sottoscrizione dell'atto di designazione e con cadenza almeno annuale o ogni qualvolta se ne verifichi la necessità alla Regione Lazio gli estremi identificativi dei soggetti nominati Amministratori di Sistema? | | | |
| E16 | Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS? | | | |
| E17 | Sono state adottate idonee misure per consentire di mettere a disposizione del Titolare e del RPD della Regione Lazio le informazioni relative ai <i>log</i> delle operazioni per un periodo di 6 mesi, qualora necessario? | | | |
| F | PRIVACY BY DESIGN E BY DEFAULT | SI | NO | N/A |
| F1 | Sono state adottate le politiche aziendali di protezione dati fin dalla progettazione (<i>privacy by design</i>)? | | | |
| F2 | È stato adottato sistema di monitoraggio delle politiche aziendali di <i>privacy by design</i> e <i>by default</i> affinché le stesse possano adeguarsi ai mutamenti tecnologici e all'insorgere di nuovi rischi? | | | |
| F3 | Sono state eseguite le valutazioni del rischio per ciascun trattamento? | | | |
| F4 | Sono state strutturate le operazioni in modo da minimizzare il trattamento dei dati personali? | | | |
| F5 | Sono state adottate tutte le misure necessarie per perseguire la massima trasparenza dei trattamenti di dati personali rendendo accessibile agli interessati idonea documentazione? | | | |
| G | MISURE DI SICUREZZA | SI | NO | N/A |
| G1 | Sono stati definiti i ruoli e le responsabilità relativi al trattamento dei dati personali? | | | |
| G2 | I soggetti di cui alla domanda G1 agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali? | | | |
| G3 | Sono state messe in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio? | | | |
| G4 | In caso di risposta affermativa alla domanda G3, le misure adottate comprendono: | | | |
| G4.1 | la pseudonimizzazione e/o la cifratura dei dati personali? | | | |
| G4.2 | misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento? | | | |
| G4.3 | misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico? | | | |
| G4.4 | procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento? | | | |
| G5 | Sono state predisposte misure tecniche che consentono l'accesso ai dati personali unicamente ai soggetti autorizzati? | | | |
| G6 | Sono state adottate almeno le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID del 18 aprile 2017, n. 2/2017? | | | |
| G7 | È stata predisposta 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? | | | |
| G12 | È prevista la vigilanza di un ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)? | | | |
| G13 | Gli operatori autorizzati possono accedere ai dati trattati con strumenti informatici soltanto dopo almeno uno o due processi di autenticazione (ad esempio il primo accesso al sistema operativo e il secondo accesso all'applicativo specifico)? | | | |
| G14 | Gli operatori autorizzati utilizzano credenziali di accesso individuali? | | | |
| G15 | Gli operatori autorizzati utilizzano dispositivi personali (PC portatili, tablet, smartphone, etc) per il trattamento dei dati? | | | |

| | | | | |
|----------|---|-----------|-----------|------------|
| G16 | L'accesso ai collegamenti VPN avviene dopo l'autenticazione a due fattori di cui uno è OTP? | | | |
| G17 | È presente una procedura interna, nel caso sia permesso ai soggetti incaricati l'utilizzo di risorse informatiche (es. PC, Tablet, smartphone) di proprietà di terzi? | | | |
| G18 | I sistemi informativi sono gestiti in proprio? | | | |
| G19 | In caso di risposta affermativa alla domanda G18: | | | |
| G19.1 | è installato sui dispositivi un sistema antivirus e <i>antimalware</i> aggiornato? | | | |
| 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 elaborazione e conservazione dei dati? | | | |
| G19.10 | è presente un impianto antintrusione? | | | |
| G19.11 | sono presenti delle procedure per l'accesso controllato dei visitatori? | | | |
| G19.12 | sono presenti dei sistemi di valutazione interni delle misure di sicurezza? | | | |
| G19.13 | sono presenti i sistemi a valutazione esterna (certificazione)? | | | |
| G19.14 | sono stati adottati i sistemi di crittografia per proteggere i dati memorizzati? | | | |
| G19.15 | sono stati adottati i sistemi di crittografia per proteggere i dati in transito? | | | |
| G19.16 | è presente di un SOC? | | | |
| G19.17 | è presente sistema SIEM? | | | |
| G19.18 | è prevista una regolare formazione degli operatori sui temi dell'utilizzo sicuro del Sistema? | | | |
| G19.19 | sono protette le connessioni ad Internet con sistemi di <i>firewall</i> , <i>intrusion detenction sistem</i> ecc.? | | | |
| G19.20 | Sono in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni tecniche o di compatibilità con sistemi <i>legacy</i>)? | | | |
| G19.21 | nell'ambito di test di sviluppo del software, sono usati dati anonimizzati? | | | |
| G19.22 | sono utilizzati ambienti di sviluppo software, test, collaudo e di produzione fisicamente e logicamente separati? | | | |
| G20 | I sistemi utilizzati sono gestiti da terzi? | | | |
| G21 | In caso di risposta affermativa alla domanda G20 si è certi che il soggetto terzo: | | | |
| G21.1 | abbia installato sui dispositivi un sistema antivirus e <i>antimalware</i> aggiornato? | | | |
| G21.2 | conservi i dati in <i>tenant</i> diversi e separati per ciascun Titolare che li ha rispettivamente forniti? | | | |
| G21.3 | provveda ad aggiornare costantemente il Sistema Operativo installato sugli elaboratori elettronici? | | | |
| G21.4 | disponga di una mappatura del proprio sistema informatico (hardware, software, dati, procedure)? | | | |
| G21.5 | disponga di un Piano di Continuità Operativa? | | | |
| G21.6 | effettui con cadenza temporale programmata test sul Piano di Continuità Operativa? | | | |
| G21.7 | disponga di un Piano di <i>Disaster Recovery</i> ? | | | |
| G21.8 | effettui con cadenza temporale programmata <i>penetration test</i> sul sistema di elaborazione dei dati? | | | |
| G21.9 | sia dotato di un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di elaborazione e conservazione dei dati? | | | |
| G21.10 | sia dotato di impianto antintrusione? | | | |
| G21.11 | sia dotato di procedure per l'accesso controllato dei visitatori? | | | |
| G21.12 | sia dotato di sistemi di valutazione interni delle misure di sicurezza? | | | |
| G21.13 | sottoponga i sistemi 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 <i>firewall</i> , <i>intrusion detenction sistem</i> ecc.? | | | |
| G21.20 | non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni tecniche o di compatibilità con sistemi <i>legacy</i>)? | | | |
| G21.21 | nell'ambito di test di sviluppo del software, usi dati anonimizzati? | | | |
| G21.22 | utilizzi ambienti di sviluppo software, test, collaudo e di produzione fisicamente e logicamente separati? | | | |
| H | PROCEDURE DI GESTIONE DEL SISTEMA INFORMATIVO AZIENDALE | SI | NO | N/A |
| H1 | Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale? | | | |
| H2 | In caso di risposta affermativa alla domanda H1: | | | |
| H2.1 | è conforme a standard internazionali? | | | |
| H2.2 | prevede regole per la gestione delle credenziali di accesso ai database? | | | |
| H2.3 | prevede regole per la gestione delle password e per l'accesso alle applicazioni? | | | |
| H2.4 | prevede regole per la gestione degli accessi ad Internet? | | | |
| H2.5 | prevede regole per la gestione degli accessi a <i>social media</i> (es: <i>Facebook</i> , <i>You Tube</i> , <i>Twitter</i> ecc)? | | | |
| H2.6 | prevede regole per la gestione e l'utilizzo della posta elettronica? | | | |

| | | | | |
|----------|---|-----------|-----------|------------|
| H2.7 | prevede regole per la gestione dei diritti di accesso ai dati? | | | |
| H2.8 | prevede regole per la gestione degli incidenti informatici? | | | |
| H2.9 | prevede regole per l'assistenza agli utenti? | | | |
| H2.10 | prevede regole per la protezione antivirus? | | | |
| H2.11 | prevede regole per la gestione dei dispositivi mobili utilizzati per il trattamento dei dati (PC portatili, smartphone, tablet, chiavi USB, dischi esterni di memorizzazione dei dati)? | | | |
| H2.12 | prevede regole per autorizzare i dipendenti a trasferire, archiviare o trattare dati personali al di fuori dei locali dell'organizzazione? | | | |
| H2.13 | prevede regole per il salvataggio di backup dei dati? | | | |
| H2.14 | prevede regole per la gestione delle stampe protette? | | | |
| H2.15 | prevede regole per la custodia e gestione degli archivi cartacei? | | | |
| I | DATA BREACH | SI | NO | N/A |
| I1 | È stata adottata una procedura per la gestione delle violazioni di dati personali (<i>data breach</i>)? | | | |
| I2 | Sono state predisposte misure organizzative idonee a garantire la tempestiva informazione al Titolare ed al RPD della Regione Lazio, (entro 24 ore dall'avvenuta conoscenza dell'evento), di ogni violazione di dati personali (<i>data breach</i>)? | | | |
| I3 | Sono state adottate misure organizzative idonee a garantire che l'informazione sulla violazione dei dati personali (<i>data breach</i>), sia corredata da tutta la documentazione utile per permettere al Titolare la tempestiva valutazione sulla necessità di notifica di violazione all'Autorità Garante per la protezione dei dati personali e/o di comunicazione agli interessati, entro i termini stabiliti dal RGPD? | | | |
| I4 | Sono stati subiti attacchi informatici con violazione di dati personali? | | | |
| I5 | Sono stati notificati nell'ultimo anno violazioni di dati personali al Garante? | | | |
| L | VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI | SI | NO | N/A |
| L1 | Sono state adottate misure tecniche ed organizzative idonee a garantire adeguata assistenza al Titolare nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'articolo 35 del RGPD, qualora lo stesso ne faccia richiesta? | | | |
| M | RICORSO AD ALTRO RESPONSABILE (di seguito SUB-RESPONSABILE) | SI | NO | N/A |
| M1 | È stato effettuato ricorso ad altro/i responsabile/i (sub-responsabili) per gestire le attività di trattamento? | | | |
| M2 | In caso di risposta affermativa alla domanda M1: | | | |
| M2.1 | È stata rilasciata autorizzazione scritta, specifica o generale, del Titolare del Trattamento? | | | |
| M2.2 | È stato informato il Titolare del trattamento di eventuali modifiche riguardanti l'aggiunta di altri sub-responsabili o la sostituzione sub-responsabili già nominati? | | | |
| M2.3 | La nomina del sub-responsabile è avvenuta mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri contenente gli stessi obblighi in materia di protezione dei dati contenuti nel contratto (o in altro atto giuridico) tra il Titolare del trattamento e il Responsabile del trattamento? | | | |
| M2.4 | Nel contratto (o altro atto giuridico) di nomina è stato previsto che il sub-responsabile fornisca sufficienti garanzie per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del RGPD? | | | |
| M2.5 | Il sub-responsabile detiene un registro con le medesime caratteristiche formali ed i medesimi contenuti 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-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 |
| N1 | Sono state adottate misure tecniche ed organizzative idonee a garantire la cancellazione o la restituzione di tutti i dati personali nei termini stabiliti per la prestazione dei servizi o, comunque, a richiesta del Titolare? | | | |
| N2 | È presente una procedura operativa per la dismissione dei supporti dei dati? | | | |
| N3 | Sono presenti i dispositivi per la distruzione dei documenti cartacei? | | | |
| O | TRASFERIMENTO DI DATI PERSONALI VERSO UN PAESE TERZO O UN'ORGANIZZAZIONE INTERNAZIONALE | SI | NO | N/A |
| O1 | Sono effettuati trasferimenti di dati personali verso Paesi terzi o organizzazioni al di fuori dello Spazio Economico Europeo? | | | |
| O2 | In caso di risposta affermativa alla domanda O1: | | | |
| O2.1 | è stata ottenuta l'autorizzazione scritta da parte del Titolare? | | | |
| O2.2 | sono state adottate idonee misure per il rispetto del Capo V (artt. 44 - 50) del RGPD? | | | |
| P | CODICI DI CONDOTTA E CERTIFICAZIONI | SI | NO | N/A |
| P1 | è prevista l'adesione a un codice di condotta ai sensi dell'art. 40 del RGPD? | | | |
| P2 | Si è in possesso della certificazione ISO 9001? | | | |
| P3 | Si è in possesso della certificazione ISO 27001? | | | |
| P4 | è presente altra certificazione rilasciata da organismi di certificazione di cui all'articolo 43 del RGPD o dall'autorità di controllo, come previsto dall'art. 42 del RGPD, che dimostri la conformità al RGPD? | | | |

| Q | ESERCIZIO DEI DIRITTI DEGLI INTERESSATI | SI | NO | N/A |
|------|--|----|----|-----|
| Q1 | Sono state adottate procedure atte a consentire l'esercizio dei diritti degli interessati? | | | |
| Q2 | In caso di risposta affermativa alla domanda Q1 sono previste procedure per: | | | |
| Q2.1 | la limitazione del trattamento? | | | |
| Q2.2 | la portabilità dei dati? | | | |
| Q2.3 | la cancellazione dei dati su richiesta dell'interessato? | | | |
| Q2.4 | la cancellazione dei dati al termine del periodo previsto? | | | |
| Q2.5 | l'estrazione dei dati su richiesta dell'interessato? | | | |
| Q2.6 | la rettifica dei dati? | | | |
| Q2.7 | la gestione dell'opposizione al trattamento? | | | |
| Q3 | Sono state adottate misure tecniche ed organizzative idonee ad assistere il Titolare nel dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui agli articoli da 15 a 22 del RGPD? | | | |
| Q4 | Sono state ricevute istanze degli interessati in esercizio ai diritti di cui agli articoli da 15 a 22 del RGPD? | | | |
| Q5 | In caso di risposta affermativa alla domanda Q4: | | | |
| Q5.1 | è stata effettuata tempestiva comunicazione scritta al Titolare e al RPD della Regione Lazio, allegando copia della richiesta? | | | |
| Q5.2 | è stato effettuato il coordinamento con il Titolare e con il RPD della Regione Lazio al fine di soddisfare le richieste? | | | |
| R | FUNZIONI CRITTOGRAFICHE - CONSERVAZIONE DELLE PASSWORD | SI | NO | N/A |
| R1 | È utilizzato un sistema di autenticazione federato (es. LDAP, Spid, ecc.)? | | | |
| R2 | In caso di risposta negativa alla domanda R1: | | | |
| R2.1 | Sono state adottate le misure tecniche previste nelle <i>Linee Guida Funzioni Crittografiche – Conservazione delle Password</i> approvate con provvedimento del Garante registro n. 594 del 7 dicembre 2023 al fine di proteggere in modo efficace le password e conservarle nell'ambito di sistemi di autenticazione informatica, o di altri sistemi, secondo le istruzioni impartite dal Titolare? | | | |
| R3 | In caso di risposta affermativa alla domanda R2.1: | | | |
| R3.1 | Sono state adottate totalmente le misure tecniche previste? | | | |
| R3.2 | Sono state adottate parzialmente le misure tecniche previste? | | | |
| R3.3 | Sono state fornite idonee istruzioni agli Amministratori di sistema? | | | |
| R3.4 | Sono state fornite idonee istruzioni ai sub-responsabili ove nominati? | | | |
| R3.5 | In caso di affidamenti di nuovi servizi, è stato previsto previsto l'inserimento di apposite clausole nei capitolati tecnici di gara? | | | |
| R4 | In caso di risposta negativa alla domanda R2.1: | | | |
| R4.1 | Sono state comunicate la circostanze al Titolare del trattamento? | | | |
| R4.2 | È possibile comprovare che le misure tecniche adottate garantiscano comunque un livello di sicurezza adeguato al rischio per i diritti e le libertà delle persone fisiche? | | | |
| R4.3 | nel determinare il periodo di conservazione delle password, è previsto l'adeguato alle indicazioni sui criteri da utilizzare fornite dal Garante nel provvedimento registro n. 594 del 7 dicembre 2023? | | | |
| R4.4 | le password sono tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per verificare l'identità degli utenti ai fini dell'accesso a sistemi informatici o servizi online? | | | |
| R4.5 | le password sono tempestivamente cancellate, anche in modo automatico, laddove non siano più necessarie per garantirne la sicurezza dei sistemi informatici o servizi online? | | | |
| R4.6 | le password sono tempestivamente cancellate, anche in modo automatico in caso di cessazione dei sistemi informatici o servizi online? | | | |
| R4.7 | le password sono tempestivamente cancellate, anche in modo automatico in caso di disattivazione delle relative credenziali di autenticazione? | | | |
| S | REQUISITI GENERALI DI SICUREZZA (Linee Guida Agid_ Sicurezza nel procurement ICT) | SI | NO | N/A |
| S1 | È effettuato annualmente un audit sul sistema di sicurezza da una società specializzata scelta previa approvazione della stazione appaltante? | | | |
| S2 | Il personale che presta supporto operativo nella sicurezza, possiede le necessarie certificazioni? | | | |
| S3 | Sono condivise le informazioni necessarie per il monitoraggio della qualità e della sicurezza? | | | |
| S4 | In caso di risposta affermativa alla domanda S3: | | | |
| S4.1 | Sono state pubblicate dette informazioni all'interno del portale della fornitura? | | | |
| S5 | È stata sottoscritta una clausola di non divulgazione (NDA) relativa ai dati e alle informazioni dell'Amministrazione Appaltante? | | | |
| S6 | Le soluzioni e i servizi di sicurezza proposti sono aggiornati da un punto di vista tecnologico? | | | |
| S7 | Le soluzioni e i servizi di sicurezza proposti sono conformi alle normative e agli standard di riferimento? | | | |
| S8 | Le soluzioni e i servizi di sicurezza proposti sono adattabili alle normative future senza oneri aggiuntivi? | | | |
| T | REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI SVILUPPO APPLICATIVO | SI | NO | N/A |
| T1 | Sono effettuate forniture di servizi di sviluppo applicativo? | | | |
| T2 | In caso di risposta affermativa alla domanda T1: | | | |
| T2.1 | In fase di progettazione e codifica, sono implementate le specifiche di sicurezza nel codice e nella struttura della base dati, con particolare riferimento alle "Linee Guida per lo sviluppo del software sicuro" di AgID? | | | |

| | | | | |
|------|---|-----------|-----------|------------|
| T3 | È stata rilasciata tutta la documentazione necessaria all'Amministrazione al termine del progetto, incluso quanto riguarda la sicurezza? | | | |
| U | REQUISITI SPECIFICI PER FORNITURE DI OGGETTI CONNESSI IN RETE | SI | NO | N/A |
| U1 | Sono effettuate forniture di oggetti connessi in rete? | | | |
| U2 | In caso di risposta affermativa alla domanda T1: | | | |
| U2.1 | Sono utilizzati protocolli sicuri e cifrati (HTTPS,SSH v2, ecc.)? | | | |
| U2.2 | È effettuato il filtraggio degli indirizzi IP? | | | |
| U2.3 | Sono offerti processi, unità organizzative e strumenti dedicati alla gestione delle vulnerabilità scoperte sui prodotti oggetto della fornitura? | | | |
| V | REQUISITI SPECIFICI PER FORNITURE DI SERVIZI DI GESTIONE REMOTA | SI | NO | N/A |
| V1 | Sono effettuate forniture di servizi di gestione remota? | | | |
| V2 | In caso di risposta affermativa alla domanda V1 | | | |
| V2.1 | Sono utilizzati meccanismi che permettano di garantire l'integrità di quanto trasmesso? | | | |
| V3 | In caso di necessità, da parte degli operatori, di accesso a Internet, è utilizzato un proxy centralizzato e dotato di configurazione? | | | |
| V4 | Su richiesta dell'amministrazione, è effettuata la consegna alla stessa dei log di sistema generati dai dispositivi di sicurezza utilizzati, almeno in formato CSV o TXT? | | | |
| V5 | In caso di risposta affermativa alla domanda V4 | | | |
| V5.1 | Sono inviati i log all'amministrazione entro il giorno successivo a quello in cui è avvenuta la richiesta? | | | |
| V6 | è monitorata la pubblicazione di upgrade/patch/hotfix necessari a risolvere eventuali vulnerabilità presenti nei dispositivi utilizzati per erogare i servizi e nelle infrastrutture gestite? | | | |