# REGIONE LAZIO

## Assessorato Lavoro, Scuola, Formazione, Ricerca, Merito e Urbanistica

***Direzione Regionale Istruzione,***
***Formazione e Politiche per l'Occupazione***

Programma Fondo Sociale Europeo Plus (FSE+) 2021- 2027
Obiettivo di Policy 4 "Un'Europa più sociale"
Regolamento (UE) n. 2021/1060
Regolamento (UE) n. 2021/1057

Priorità: 4. Giovani (Occupazione giovanile)

Obiettivo specifico: ESO4.1. Migliorare l'accesso all'occupazione e le misure di attivazione per tutte le persone in cerca di lavoro, in particolare i giovani, soprattutto attraverso l'attuazione della garanzia per i giovani, i disoccupati di lungo periodo e i gruppi svantaggiati nel mercato del lavoro, nonché delle persone inattive, anche mediante la promozione del lavoro autonomo e dell'economia sociale

Avviso per l'individuazione di soggetti interessati ad erogare interventi di formazione di base e trasversale di cui al Regolamento regionale 29 marzo 2017 n.7 nell'ambito di contratti di apprendistato professionalizzante ex art. 44 D.lgs n. 81/2015 – Terza edizione

**ALLEGATO M: QUESTIONARIO DI VALUTAZIONE DEL RESPONSABILE ED ISTRUZIONI**

| ISTRUZIONI PER LA COMPILAZIONE | |
|---|---|
| **ANAGRAFICA** | L'anagrafica va compilata in ogni sua parte |
| **ANAGRAFICA - PERIODO DI RIFERIMENTO** | È 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. |
| **QUESTIONARIO - UTILIZZO DELLA COLONNA N/A** | Il campo N/A deve essere valorizzato esclusivamente in caso di fattispecie non applicabile. |
| **QUESTIONARIO- SEZIONE L - 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). 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 | Il Responsabile effettua le operazioni di trattamento attenendosi alle disposizioni operative del Titolare? | | | |
| A2 | Il Responsabile, su indicazione del Titolare, sta effettuando o ha effettuato trattamenti su dati personali diversi rispetto a quelli normalmente eseguiti nell'ambito della designazione? | | | |
| A3 | In caso di risposta affermativa alla domanda A2, il Responsabile ha provveduto, all'insorgere dell'esigenza, ad informare preventivamente il Titolare del trattamento e il RPD della Regione Lazio? | | | |
| A4 | Il Responsabile, di propria iniziativa e/o per proprie finalità, sta effettuando o ha effettuato 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 | Il Responsabile ha 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 | Il Responsabile ha designato un proprio 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 | Il Responsabile si avvale di soggetti autorizzati al trattamento dati all'interno della propria struttura? | | | |
| D2 | In caso di risposta affermativa alla domanda D1: | | | |
| D2.1 | sono stati autorizzati con atto formale? | | | |

| | | | | |
|---|---|---|---|---|
| D2.2 | sono stati adeguatamente istruiti sul tema della protezione dei dati personali? | | | |
| D2.3 | sono previste attività formative con aggiornamenti periodici in tema di protezione di dati personali? | | | |
| D2.4 | le istruzioni operative impartite ai soggetti autorizzati sono idonee a garantire il rispetto delle finalità per cui i dati sono stati raccolti e trattati? | | | |
| D2.5 | i soggetti autorizzati al trattamento sono vincolati ad un obbligo, legalmente assunto, di riservatezza? | | | |
| D3 | Alcune attività vengono svolte in modalità di "lavoro agile"? | | | |
| D4 | Il "lavoro agile" è disciplinato da regolamenti e/o procedure interne? | | | |
| **E** | **AMMINISTRATORI DI SISTEMA** | **SI** | **NO** | **N/A** |
| E1 | Sono stati individuati i soggetti ai quali affidare il ruolo di Amministratori di Sistema (*System Administrator*), Amministratori di Base Dati (*Database Administrator*), Amministratori di Rete (*Network Administrator*) e/o Amministratori di *Software* complessi? | | | |
| E2 | In caso di risposta affermativa alla domanda E1: | | | |
| E2.1 | Sono stati sottoscritti appositi atti di designazione individuale? | | | |
| E2.2 | Sono state impartire adeguate istruzioni ai designati secondo i ruoli assegnati? | | | |
| E2.3 | Il Responsabile ha adottato misure di controllo e di vigilanza sul loro operato? | | | |
| E2.4 | Tiene costantemente aggiornato l'elenco degli ADS con l'indicazione delle relative utenze? | | | |
| E2.5 | Le nomine degli Amministratori sono aggiornate ad ogni modifica della normativa vigente? | | | |
| E3 | È stata assegnata ai suddetti soggetti una *user id* agevolmente riconducibile all'identità degli Amministratori? | | | |
| E4 | In caso di risposta affermativa alla domanda E3 sono rispettate le seguenti regole? | | | |
| E4.1 | divieto di assegnazione di *user id* generiche e già attribuite anche in tempi diversi; | | | |
| E4.2 | utilizzo di utenze amministrative anonime, quali "*root*" di *Unix o* "*Administrator*" di *Windows*, solo per situazioni di emergenza; | | | |
| E4.3 | le credenziali utilizzate assicurano sempre l'imputabilità delle operazioni a chi ne fa uso; | | | |
| E4.4 | disattivazione delle *user id* attribuite agli Amministratori che, per qualunque motivo, non necessitano più di accedere ai dati. | | | |
| E5 | Le password associate alle *user id* assegnate agli Amministratori prevedono il rispetto delle seguenti regole? | | | |
| E5.1 | *password* con lunghezza minima di almeno 14 caratteri, qualora l'autenticazione a più fattori non sia supportata; | | | |
| E5.2 | cambio *password* alla prima connessione e successivamente almeno ogni 30 giorni (*password again*); | | | |

| | | | | |
|---|---|---|---|---|
| E5.3 | le *password* devono differire dalle ultime 5 utilizzate (*password history*); | | | |
| E5.4 | le *password* sono conservate in modo da garantirne disponibilità e riservatezza; | | | |
| E5.5 | registrazione di tutte le immissioni errate di *password*; | | | |
| E6 | Gli *account* degli Amministratori sono bloccati dopo un numero massimo di tentativi falliti di *login*, ove tecnicamente possibile? | | | |
| E7 | L'archiviazione di *password* o codici PIN su qualsiasi supporto fisico avvenga è protetta da sistemi di cifratura? | | | |
| E8 | È assicurata la completa distinzione, in capo al medesimo utente, tra utenze privilegiate (amministratore) e non privilegiate, alle quali devono corrispondere credenziali diverse? | | | |
| E9 | I profili di accesso per le utenze di ADS rispettano il principio del *need-to-know*, ovvero che non siano attribuiti diritti oltre a quelli realmente necessari per eseguire le attività di lavoro? | | | |
| E10 | I sistemi sono dotati di strumenti automatici tipo *alert* che si attivano ad esempio quando viene aggiunta una utenza amministrativa e/o quando sono aumentati i diritti di una utenza amministrativa già attiva? | | | |
| E11 | Sono stati adottati sistemi di registrazione degli accessi logici (*log*) degli Amministratori ai sistemi? | | | |
| E12 | La conservazione dei registri degli accessi logici è garantita per un periodo non inferiore a 6 mesi? | | | |
| E13 | In caso di utilizzo di sistemi messi a disposizione dalla Regione, è stato comunicato agli Amministratori che la Regione stessa procederà alla registrazione e conservazione dei *log*? | | | |
| E14 | Sono state adottate idonee misure finalizzate ad obbligare l'Amministratore ad accedere ai sistemi con una utenza normale e solo successivamente eseguire i singoli comandi come ADS? | | | |
| E15 | Sono state comunicati al momento della sottoscrizione dell'atto di designazione e con cadenza almeno annuale o ogni qualvolta se ne verifichi la necessità alla Regione Lazio gli estremi identificativi dei soggetti nominati Amministratori di Sistema? | | | |
| E16 | Sono state eseguite, con cadenza almeno annuale, le attività di verifica dell'operato degli ADS? | | | |
| E17 | Sono state adottate idonee misure per consentire di mettere a disposizione del Titolare e del RPD della Regione Lazio le informazioni relative ai *log* delle operazioni per un periodo di 6 mesi, qualora necessario? | | | |
| **F** | **MISURE DI SICUREZZA** | **SI** | **NO** | **N/A** |
| F1 | Il Responsabile ha definito i ruoli e le responsabilità relativi al trattamento dei dati personali? | | | |
| F2 | I soggetti di cui al alla domanda F1 agiscono secondo procedure interne definite per la gestione degli adempimenti sulla protezione dei dati personali? | | | |

| | | | | |
|---|---|---|---|---|
| F3 | Il Responsabile ha messo in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio? | | | |
| F4 | In caso di risposta affermativa alla domanda F3 se del caso, le misure adottate comprendono: | | | |
| F4.1 | La pseudonimizzazione e/o la cifratura dei dati personali? | | | |
| F4.2 | Misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento? | | | |
| F4.3 | Misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico? | | | |
| F4.4 | Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento? | | | |
| F5 | Il Responsabile ha predisposto misure tecniche che consentano l'accesso ai dati personali unicamente ai soggetti autorizzati? | | | |
| F6 | Il Responsabile ha adottato almeno le misure minime di sicurezza ICT per le PP.AA. di cui alla circolare AgID del 18 aprile 2017, n. 2/2017? | | | |
| F7 | Il Responsabile ha predisposto idonea documentazione tecnica relativa alle misure di sicurezza in atto? | | | |
| F8 | In caso di risposta affermativa alla domanda F7: | | | |
| F.8.1 | la documentazione tecnica tiene traccia delle eventuali modifiche delle misure di sicurezza in atto? | | | |
| F.8.2 | la documentazione è disponibile e producibile a richiesta del Titolare? | | | |
| F9 | Il Responsabile ha adottato un approccio alla sicurezza dei dati basato sul rischio? | | | |
| F10 | Il Responsabile è dotato di impianto antintrusione? | | | |
| F11 | Il Responsabile è dotato di procedure di controllo per l'accesso dei visitatori? | | | |
| F12 | Il Responsabile è sottoposto alla vigilanza di un'ente specifico? (ad es. AgID, ACN, Banca d'Italia, Federazioni di categoria, associazioni ecc)? | | | |
| F13 | 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)? | | | |
| F14 | Gli operatori autorizzati utilizzano credenziali di accesso individuali? | | | |
| F15 | Gli operatori autorizzati utilizzano dispositivi personali (PC portatili, tablet, smartphone, etc) per il trattamento dei dati? | | | |
| F16 | L'accesso ai collegamenti VPN avviene dopo l'autenticazione a due fattori di cui uno è OTP? | | | |
| F17 | Il Responsabile, nel caso sia permesso ai soggetti incaricati l'utilizzo di risorse informatiche (es. PC, Tablet, smartphone) di proprietà di terzi, si è dotato di una procedura interna? | | | |

| | | | | |
|---|---|---|---|---|
| F18 | I sistemi informativi sono gestiti in proprio? | | | |
| F19 | In caso di risposta affermativa alla domanda F18 il Responsabile: | | | |
| F19.1 | ha installato sui dispositivi un sistema antivirus e *antimalware* aggiornato? | | | |
| F19.2 | conserva i dati in *tenant* diversi e separati per ciascun Titolare che li ha rispettivamente forniti? | | | |
| F19.3 | provvede ad aggiornare costantemente il Sistema Operativo installato sugli elaboratori elettronici? | | | |
| F19.4 | dispone di una mappatura del proprio sistema informatico (hardware, software, dati, procedure)? | | | |
| F19.5 | dispone di un Piano di Continuità Operativa? | | | |
| F19.6 | effettua con cadenza temporale programmata test sul Piano di Continuità Operativa? | | | |
| F19.7 | dispone di un Piano di *Disaster Recovery*? | | | |
| F19.8 | effettua con cadenza temporale programmata *penetration test* sul sistema di elaborazione dei dati? | | | |
| F19.9 | è dotato di un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di elaborazione e conservazione dei dati? | | | |
| F19.10 | è dotato di impianto antintrusione? | | | |
| F19.11 | è dotato di procedure per l'acceso controllato dei visitatori? | | | |
| F19.12 | è dotato di sistemi di valutazione interni delle misure di sicurezza? | | | |
| F19.13 | sottopone i istemi a valutazione esterna (certificazione)? | | | |
| F19.14 | ha adottato sistemi di crittografia per proteggere i dati memorizzati? | | | |
| F19.15 | ha adottato sistemi di crittografia per proteggere i dati in transito? | | | |
| F19.16 | è dotato di un SOC? | | | |
| F19.17 | è dotato di un sistema SIEM? | | | |
| F19.18 | procede alla regolare formazione degli operatori sui temi dell'utilizzo sicuro del Sistema? | | | |
| F19.19 | ha protetto le connessioni ad Internet con sistemi di *firewall*, *intrusion detenction sistem* ecc.? | | | |
| F19.20 | non ha in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni tecniche o di compatibilità con sistemi *legacy*)? | | | |
| F19.21 | nell'ambito di test di sviluppo del software, usa dati anonimizzati? | | | |
| F19.22 | utilizza ambienti di sviluppo software, test, collaudo e di produzione fisicamente e logicamente separati? | | | |
| F20 | I sistemi del Responsabile sono gestiti da terzi? | | | |
| F21 | In caso di risposta affermativa alla domanda F20 il Responsabile si è assicurato che il soggetto terzo: | | | |
| F21.1 | abbia installato sui dispositivi un sistema antivirus e antimalware aggiornato? | | | |

| | | | | |
|---|---|---|---|---|
| F21.2 | conservi i dati in tenant diversi e separati per ciascun Titolare che li ha rispettivamente forniti? | | | |
| F21.3 | provveda ad aggiornare costantemente il Sistema Operativo installato sugli elaboratori elettronici? | | | |
| F21.4 | disponga di una mappatura del proprio sistema informatico (hardware, software, dati, procedure)? | | | |
| F21.5 | disponga di un Piano di Continuità Operativa? | | | |
| F21.6 | effettui con cadenza temporale programmata test sul Piano di Continuità Operativa? | | | |
| F21.7 | disponga di un Piano di Disaster Recovery? | | | |
| F21.8 | effettui con cadenza temporale programmata penetration test sul sistema di elaborazione dei dati? | | | |
| F21.9 | sia dotato di un impianto di videosorveglianza negli spazi dove sono collocati dispositivi di elaborazione e conservazione dei dati? | | | |
| F21.10 | sia dotato di impianto antintrusione? | | | |
| F21.11 | sia dotato di procedure per l'acceso controllato dei visitatori? | | | |
| F21.12 | sia dotato di sistemi di valutazione interni delle misure di sicurezza? | | | |
| F21.13 | sottoponga i istemi a valutazione esterna (certificazione)? | | | |
| F21.14 | abbia adottato sistemi di crittografia per proteggere i dati memorizzati? | | | |
| F21.15 | abbia adottato sistemi di crittografia per proteggere i dati in transito? | | | |
| F21.16 | sia dotato di un SOC? | | | |
| F21.17 | sia dotato di un sistema SIEM? | | | |
| F21.18 | proceda alla regolare formazione degli operatori sui temi dell'utilizzo sicuro del Sistema? | | | |
| F21.19 | protegga le connessioni ad Internet con sistemi di firewall, intrusion detenction sistem ecc.? | | | |
| F21.20 | non abbia in uso dispositivi (PC o Server) dotati di sistemi operativi obsoleti (ad esempio per ragioni tecniche o di compatibilità con sistemi legacy)? | | | |
| F21.21 | nell'ambito di test di sviluppo del software, usi dati anonimizzati? | | | |
| F21.22 | utilizzi ambienti di sviluppo software, test, collaudo e di produzione fisicamente e logicamente separati? | | | |
| **G** | **PROCEDURE DI GESTIONE DEL SISTEMA INFORMATIVO AZIENDALE** | **SI** | **NO** | **N/A** |
| G1 | Esiste una procedura per la gestione e l'utilizzo del Sistema Informativo Aziendale? | | | |
| G2 | In caso di risposta affermativa alla domanda G1: | | | |
| G2.1 | è conforme a standard internazionali? | | | |
| G2.2 | prevede regole per la gestione delle credenziali di accesso ai database? | | | |

| | | | | |
|---|---|---|---|---|
| G2.3 | prevede regole per la gestione delle password e per l'accesso alle applicazioni? | | | |
| G2.4 | prevede regole per la gestione degli accessi ad Internet? | | | |
| G2.5 | prevede regole per la gestione degli accessi a *social media* (es: *Facebook*, *You Tube, Twitter* ecc)? | | | |
| G2.6 | prevede regole per la gestione e l'utilizzo della posta elettronica? | | | |
| G2.7 | prevede regole per la gestione dei diritti di accesso ai dati? | | | |
| G2.8 | prevede regole per la gestione degli incidenti informatici? | | | |
| G2.9 | prevede regole per l'assistenza agli utenti? | | | |
| G2.10 | prevede regole per la protezione antivirus? | | | |
| G2.11 | 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? | | | |
| G2.12 | prevede regole per autorizzare i dipendenti a trasferire, archiviare o trattare dati personali al di fuori dei locali dell'organizzazione? | | | |
| G2.13 | prevede regole per il salvataggi di backup dei dati? | | | |
| G2.14 | prevede regole per la gestione delle stampe protette? | | | |
| G2.15 | prevede regole per la custodia e gestione degli archivi cartacei? | | | |
| **H** | ***DATA BREACH*** | **SI** | **NO** | **N/A** |
| H1 | Il Responsabile ha adottato una propria procedura per la gestione delle violazioni di dati personali (*data breach*)? | | | |
| H2 | Il Responsabile ha predisposto misure organizzative idonee a garantire la tempestiva informazione al Titolare ed al RPD della Regione Lazio, (entro 24 ore dall'avvenuta conoscenza dell'evento), di ogni violazione di dati personali (*data breach*)? | | | |
| H3 | Il Responsabile ha adottato misure organizzative idonee a garantire che l'informazione sulla violazione dei dati personali (*data breach*), sia corredata da tutta la documentazione utile per permettere al Titolare la tempestiva valutazione sulla necessità di notifica di violazione all'Autorità Garante per la protezione dei dati personali e/o di comunicazione agli interessati, entro i termini stabiliti dal RGPD? | | | |
| H4 | Il Responsabile, nell'ultimo anno, è stato esente da attacchi informatici con violazione di dati personali? | | | |
| H5 | Il Responsabile ha notificato nell'ultimo anno violazioni di dati personali al Garante? | | | |
| **I** | **VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI** | **SI** | **NO** | **N/A** |
| I1 | Il Responsabile ha adottato 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? | | | |
| **L** | **RICORSO AD ALTRO RESPONSABILE (di seguito SUB-RESPONSABILE)** | **SI** | **NO** | **N/A** |

| | | | | |
|---|---|---|---|---|
| L1 | Il Responsabile ha fatto ricorso ad altro/i responsabile/i (sub-responsabili) per gestire attività di trattamento? | | | |
| L2 | In caso di risposta affermativa alla domanda L1: | | | |
| L2.1 | il Responsabile è stato preventivamente autorizzato, con autorizzazione scritta, specifica o generale, del Titolare del Trattamento? | | | |
| L2.2 | il Responsabile ha informato il Titolare del trattamento di eventuali modifiche riguardanti l'aggiunta di altri sub-responsabili o la sostituzione sub-responsabili già nominati? | | | |
| L2.3 | 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? | | | |
| L2.4 | 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? | | | |
| L2.5 | il Responsabile si è assicurato che il sub-responsabile nominato detenga un registro con le medesime caratteristiche formali ed i medesimi contenuti sopra indicati relativamente ai trattamenti di competenza? | | | |
| L2.6 | nel contratto/altro atto giuridico sono state fornite adeguate istruzioni al sub-responsabile? | | | |
| L3 | Il Responsabile effettua periodiche verifiche sull'adeguatezza delle misure tecniche e organizzative adottate dal sub-responsabile? | | | |
| **M** | **CANCELLAZIONE E/O RESTITUZIONE DEI DATI PERSONALI TRATTATI** | **SI** | **NO** | **N/A** |
| M1 | Il Responsabile ha adottato 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? | | | |
| M2 | Il Responsabile è dotato di una procedura operativa per la dismissione dei supporti dei dati? | | | |
| M3 | Il Responsabile è dotato di dispositivi per la distruzione dei documenti cartacei? | | | |
| **N** | **TRASFERIMENTO DI DATI PERSONALI VERSO UN PAESE TERZO O UN'ORGANIZZAZIONE INTERNAZIONALE** | **SI** | **NO** | **N/A** |
| N1 | Il Responsabile, per le attività che svolge per conto del Titolare, effettua trasferimenti di dati personali verso Paesi terzi o organizzazioni al di fuori dello Spazio Economico Europeo? | | | |
| N2 | In caso di risposta affermativa alla domanda N1: | | | |
| N2.1 | ha preventivamente ottenuto l'autorizzazione scritta da parte del Titolare? | | | |

| | | | | |
|---|---|---|---|---|
| N2.2 | ha adottato idonee misure per il rispetto del Capo V (artt. 44 - 50) del RGPD? | | | |
| **O** | **CODICI DI CONDOTTA E CERTIFICAZIONI** | **SI** | **NO** | **N/A** |
| O1 | Il Responsabile ha aderito a un codice di condotta ai sensi dell'art. 40 del RGPD? | | | |
| O2 | Il Responsabile è certificato ISO 9001? | | | |
| O3 | Il Responsabile è certificato ISO 27001? | | | |
| O4 | Il Responsabile è in possesso di 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? | | | |
| **P** | **ESERCIZIO DEI DIRITTI DEGLI INTERESSATI** | **SI** | **NO** | **N/A** |
| P1 | Il Responsabile ha adottato procedure atte a consentire l'esercizio dei diritti degli interessati? | | | |
| P2 | In caso di risposta affermativa alla domanda P1 sono previste procedure per: | | | |
| P2.1 | la limitazione del trattamento? | | | |
| P2.2 | la portabilità dei dati? | | | |
| P2.3 | la cancellazione dei dati su richiesta dell'interessato? | | | |
| P2.4 | la cancellazione dei dati al termine del periodo previsto? | | | |
| P2.5 | l'estrazione dei dati su richiesta dell'interessato? | | | |
| P2.6 | la rettifica dei dati? | | | |
| P2.7 | la gestione dell'opposizione al trattamento? | | | |
| P3 | Il Responsabile del Trattamento ha adottato 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? | | | |
| P4 | Il Responsabile ha ricevuto istanze degli interessati in esercizio ai diritti di cui agli articoli da 15 a 22 del RGPD? | | | |
| P5 | In caso di risposta affermativa alla domanda P4: | | | |
| P5.1 | ne ha dato tempestiva comunicazione scritta al Titolare e al RPD della Regione Lazio, allegando copia della richiesta? | | | |
| P5.2 | si è coordinato con il Titolare e con il RPD della Regione Lazio al fine di soddisfare le richieste? | | | |