Allegato G

Disciplina dei rapporti tra Regione Lazio e LAZIOCrea in materia di trattamenti di dati personali nell'ambito dei servizi affidati a quest'ultima in ordine a: istruzioni, natura e finalità del trattamento, tipo di dati personali e categorie di interessati, obblighi e diritti del titolare del trattamento, compiti e responsabilità del responsabile del trattamento in osservanza dell'articolo 28 paragrafo 3) del Regolamento Europeo n. 679/2016.

Articolo 1
Definizioni

Ai fini della presente disciplina valgono le seguenti definizioni:

- Per "Legge Applicabile" o "Normativa Privacy", si intende il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito, per brevità, "GDPR") a far data dal 25.05.2018, il D.Lgs. 196/2003 e s.m.i. e i suoi allegati (di seguito, per brevità, anche "Codice della Privacy"), nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia, anche emanata ai sensi dell'art. 13 della Legge n. 163 del 25 ottobre 2017, ivi compresi i provvedimenti dell'Autorità Garante per la Protezione dei dati personali (di seguito, per brevità, "Garante");
- per "Dati Personali": si intendono tutte le informazioni direttamente o indirettamente riconducibili ad una persona fisica così come definite ai sensi dell'art. 4 par. 1 del GDPR, che il Responsabile tratta per conto del Titolare allo scopo di fornire i Servizi di cui al Piano Operativo Annuale di riferimento;
- per "Interessato": si intende la persona fisica cui si riferiscono i Dati Personali;
- per "Servizi": si intendono i Servizi resi dal Responsabile oggetto del contratto quadro dei servizi nonché il relativo trattamento dei dati personali;
- per "Titolare": si intende, ai sensi dell'art. 4, par. 7 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Il Titolare del Trattamento è la Giunta della Regione Lazio.
- per "Responsabile del Trattamento": si intende, ai sensi dell'art. 4, par. 8 del GDPR, la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento. Il Responsabile del trattamento è LAZIOCrea;
- per "Ulteriore Responsabile": si intende la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, soggetto terzo (fornitore) rispetto alle Parti, a cui il Responsabile del trattamento, previa autorizzazione del Titolare, abbia, nei modi di cui al par. 4 dell'art. 28 del GDPR, eventualmente affidato parte dei Servizi e che quindi tratta dati personali. Ulteriore Responsabile sono in generale gli operatori economici.
- per "Misure di Sicurezza": si intendono le misure di sicurezza di all'art. 32 del GDPR;
- per "Trattamento": si intende, ai sensi dell'art. 4, par. 2 del GDPR, qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi

altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

- per “Violazione di Dati personali” (c.d. Data Breach), si intende ai sensi dell'art. 4, par. 12 del GDPR, la violazione di sicurezza che comporta anche accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati;
- per “Amministratore di Sistema” si intende la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti; è altresì considerato tale anche altra figura equiparabile dal punto di vista dei rischi relativi alla protezione dei dati, quale l’amministratore di basi di dati, l’amministratore di reti e di apparati di sicurezza e l’amministratore di sistemi software complessi utilizzati in grandi organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;
- per “Responsabile della protezione dei dati (Data Protection Officer – DPO)” si intende la figura di cui all’articolo 37 e seguenti del GDPR designato con DGR n. 230 del 15 maggio 2018.

Articolo 2

Oggetto

1. La presente disciplina regolamenta le operazioni di trattamento dei dati personali rientranti nella sfera di titolarità della Regione Lazio effettuate dalla società LAZIOcrea nell’ambito del Contratto Quadro di Servizi di cui alla DGR n. 891/2017 per i servizi riportati nel documento di programmazione definito annualmente e denominato Piano Operativo Annuale (di seguito POA).

Articolo 3

Durata e finalità

1. La presente disciplina rimarrà in vigore fino alla cessazione delle attività svolte dalla LAZIOCrea in riferimento al trattamento dei dati personali rientrati nella sfera della titolarità della Regione Lazio.
2. Resta fermo il diritto del Titolare, in qualsiasi momento, di revocare e/o modificare la nomina di LAZIOCrea quale responsabile del trattamento dei dati personali, ivi compresi i relativi compiti e responsabilità salvo ogni eventuale obbligo di legge.
3. I trattamenti dei dati personali saranno effettuati dalla LAZIOCrea per il tempo strettamente necessario al conseguimento della finalità per le quali i dati sono raccolti e successivamente trattati in relazione alle tipologie di servizio affidati attraverso il POA.

Articolo 4

Tipologie di dati e Categorie di interessati

1. LAZIOCrea per conto della Regione Lazio effettua operazioni di trattamento aventi ad oggetto tutte le categorie di dati personali rientranti nella titolarità dell’amministrazione stessa (cittadini, utenti, personale dipendente regionale, etc.) relativamente ai servizi affidati attraverso il POA.

Articolo 5

Modalità e istruzioni

1. Le modalità e le istruzioni per il Trattamento dei Dati Personali impartite dal Titolare al Responsabile sono contenute nella presente disciplina, come riportate nei successivi articoli, fermo restando quanto già previsto dal Contratto Quadro di Servizi e dal POA e potranno essere declinate dalle Direzioni competenti per materia con ulteriori e più dettagliate istruzioni in riferimento alle particolari tipologie di servizio.

Articolo 6

Obblighi e doveri del Responsabile del trattamento

1. Il Responsabile è obbligato a fornire garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che i trattamenti effettuati nell'ambito dell'erogazione dei servizi - così come specificati nel POA - soddisfi i requisiti di cui al GDPR nonché tuteli i diritti degli interessati al trattamento. In particolare, il Responsabile si impegna a mantenere una struttura ed una organizzazione adeguata per la corretta esecuzione dei servizi indicati nel POA (per sé e per i propri dipendenti e collaboratori interni ed esterni) nel rispetto delle menzionate disposizioni normative nonché nel rispetto delle istruzioni specificatamente impartite dal Titolare nel presente atto e/o di volta in volta impartite in riferimento ai singoli servizi affidati.
2. In particolare, LAZIOCrea, in qualità di Responsabile è obbligato a:
   - effettuare le operazioni di trattamento dei dati stabiliti dal Contratto Quadro di Servizi e dal POA e nel rispetto delle disposizioni normative vigenti;
   - adottare le misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio in osservanza delle disposizioni di cui agli articoli 32 e 35 del GDPR, prima dell'inizio delle attività al fine di garantire il rispetto del principio della "Protezione dei dati fin dalla progettazione e protezione predefinita" di cui all'art. 25 del GDPR, già in fase contrattuale;
   - eseguire i trattamenti connessi ai servizi erogati a supporto dell'amministrazione regionale compatibilmente e nei limiti delle finalità perseguite. Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, LAZIOCrea dovrà informare il Titolare del trattamento ed il Data Protection Officer (DPO) della Regione Lazio.
   - adottare le misure organizzative e procedurali necessarie al fine di autorizzare il personale preposto alle operazioni di trattamento nonché impartire allo stesso le necessarie istruzioni in materia di privacy nel rispetto delle disposizioni normative nonché delle condizioni e dei termini contemplati nel presente atto, ivi compresi le istruzioni impartite di volta in volta. Il Responsabile ha l'obbligo di garantire che il personale autorizzato al trattamento sia vincolato legalmente al rispetto degli obblighi di riservatezza.
   - garantire l'adozione delle misure di sicurezza di cui all'articolo 32 del GDPR. In particolare - tenuto conto dello stato dell'arte delle misure di sicurezza adottate a protezione dei trattamenti dei dati per conto della Regione Lazio come previste dal contratto vigente, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento e, sulla base delle risultanze dell'analisi dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, che derivano in particolare dalla distruzione, dalla perdita, dalla

modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati - porre in essere le opportune azioni organizzative per l'ottimizzazione di tali misure, per garantire un livello di sicurezza adeguato al rischio. Tali misure comprendono, tra le altre:

a) la cifratura dei dati personali;
b) misure idonee a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) misure idonee a garantire la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico;
d) procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

- trasmettere al Titolare del trattamento la documentazione tecnica relativa sia alle misure di sicurezza in atto sia alle modifiche in seguito applicate; inoltre renderà disponibili al Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli adempimenti normativi previsti dal GDPR, consentendo di effettuare periodicamente attività di verifica, comprese ispezioni realizzate dal Titolare stesso o da un altro soggetto da questi incaricato.
- adottare le politiche interne e impegnarsi ad attuare le misure che soddisfino i principi della protezione dei dati personali fin dalla progettazione di tali misure (privacy by design); adottare ogni misura adeguata a garantire che i dati personali siano trattati in ossequio al principio di necessità ovvero che siano trattati solamente per le finalità previste e per il tempo strettamente necessario al raggiungimento delle stesse (privacy by default).
- tenere, ai sensi dell'art. 30 del GDPR e nei limiti di quanto esso prescrive, un Registro delle attività di Trattamento effettuate sotto la propria responsabilità per conto della Regione Lazio e cooperare con il Titolare e con l'Autorità Garante per la protezione dei dati personali, laddove ne venga fatta richiesta ai sensi dell'art. 30, comma 4 del GDPR.
- assistere il Titolare, ove richiesto, nello svolgimento della valutazione d'impatto sulla protezione dei dati, conformemente a quanto prescritto dall'art. 35 del GDPR e nella eventuale consultazione del Garante per la protezione dei dati personali, prevista dall'art. 36 del GDPR.
- qualora riceva istanze degli interessati in esercizio dei loro diritti di cui dall'art. 15 all'art. 22 del GDPR:
  - dare tempestiva comunicazione scritta al Titolare e al Data Protection Officer (DPO) della Regione Lazio, allegando copia della richiesta;
  - valutare con il Titolare e con il Data Protection Officer (DPO) della Regione Lazio la legittimità delle richieste;
  - coordinarsi con il Titolare e con il Data Protection Officer (DPO) della Regione Lazio al fine di soddisfare le richieste ritenute legittime.

- garantire gli adempimenti e le incombenze anche formali verso l'Autorità Garante quando richieste e nei limiti dovuti, disponendosi a collaborare tempestivamente, per quanto di competenza, sia con il Titolare sia con l'Autorità. In particolare LAZIOcrea dovrà:
  - fornire informazioni sulle operazioni di trattamento svolte;
  - consentire l'accesso alle banche dati oggetto delle operazioni di trattamento;
  - consentire l'effettuazione di controlli;
  - mettere in atto quanto necessario per una tempestiva esecuzione dei provvedimenti inibitori, di natura temporanea.
- garantire l'applicazione di quanto disposto dal Titolare in merito alle misure di sicurezza da adottare al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, secondo quanto prescritto dagli artt. 25 e 32 del GDPR EU 2016/679 in materia di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Privacy by Design) e in materia di misure di sicurezza;
- informare il Titolare tempestivamente ove riscontri carenze sulle misure di sicurezza o su qualunque aspetto relativo ai trattamenti che dovesse comportare responsabilità penale, civile e ammnistrativa del medesimo Titolare; In particolare è tenuta altresì ad informate periodicamente il Titolare sullo stato dell'arte relativo agli obblighi e alle prescrizioni contemplate dal GDPR, segnalando contestualmente le eventuali azioni da intraprendere;
- non trasferire i dati personali verso un paese terzo o un'organizzazione internazionale, salvo che non abbia preventivamente ottenuto l'autorizzazione scritta da parte del Titolare e nel rispetto della normativa applicabile.

  In aggiunta LAZIOcrea SPA è obbligata ad adottare le ulteriori misure specifiche stabilite dal Titolare, nel rispetto del contratto vigente.

Articolo 7

Ulteriori Obblighi del Responsabile in materia di Amministratore di Sistema

1. In conformità a quanto prescritto dal Provvedimento del Garante del 27 novembre 2008 e successive modifiche ed integrazioni, ed alle Misure minime AgID relativamente alle utenze Amministrative, laddove le prestazioni contrattuali implichino l'erogazione di servizi di amministrazione di sistema, LAZIOCrea, in qualità di Responsabile del trattamento, si impegna a:
   - individuare 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 e, sulla base del successivo atto di designazione individuale, impartire le istruzioni a detti soggetti, vigilando sul relativo operato;
   - assegnare ai suddetti soggetti una *user id* che contenga riferimenti agevolmente riconducibili all'identità degli Amministratori e che consenta di garantire il rispetto delle seguenti regole:
     - divieto di assegnazione di *user id* generiche e già attribuite anche in tempi diversi;

- utilizzo di utenze amministrative anonime, quali “root” di Unix o “Administrator” di Windows, solo per situazioni di emergenza e le relative credenziali devono essere gestite in modo da assicurare l’imputabilità di chi ne fa uso;
- rimozione dei privilegi di Amministratore delle *user id* attribuite alle figure di Amministratori che non necessitano più di accedere ai dati;

- associare alle *user id* assegnate agli Amministratori una password di adeguata complessità nel rispetto delle “*best practices*” vigenti;
- assicurare la completa distinzione tra utenze privilegiate e non privilegiate di amministratore, alle quali devono corrispondere credenziali diverse;
- assicurare che i profili di accesso, in particolare per le utenze con privilegi amministrativi, rispettino il principio del need-to-know, ovvero che non siano attribuiti diritti superiori a quelli realmente necessari per eseguire le normali attività di lavoro. Le utenze con privilegi amministrativi devono essere utilizzate per il solo svolgimento delle funzioni assegnate;
- mantenere aggiornato un inventario delle utenze privilegiate (Anagrafica AdS), anche attraverso uno strumento automatico in grado di generare un alert quando è aggiunta una utenza amministrativa e quando sono aumentati i diritti di una utenza amministrativa;
- adottare sistemi di registrazione degli accessi logici (log) degli Amministratori ai sistemi e conservare gli stessi per un congruo periodo di 180 giorni;
- comunicare su richiesta annuale e/o ogni qualvolta se ne verifichi la necessità, al DPO della Regione Lazio gli estremi identificativi delle persone fisiche preposte quali Amministratori di Sistema, di Base Dati, di Rete e/o di software Complessi, specificando per ciascuno di tali soggetti:
  - il nome e cognome;
  - la *user id* assegnata agli Amministratori;
  - il ruolo degli Amministratori (ovvero di Sistema, Base Dati, di Rete e/o di Software Complessi);
  - i sistemi che gli stessi gestiscono, specificando per ciascuno il profilo di autorizzazione assegnato;
- eseguire, con cadenza almeno annuale, le attività di verifica dell’operato degli Amministratori e consentire comunque alla Regione Lazio ove ne faccia richiesta, di eseguire in proprio dette verifiche;
- nei limiti dell’incarico affidato, mettere a disposizione del Titolare e del DPO della Regione Lazio, quando formalmente richieste, le seguenti informazioni relative agli Amministratori: log-in riusciti, log-in falliti, e log-out. Tali dati dovranno essere resi disponibili per un periodo di 180 giorni;
- in caso di modifiche normative e/o regolamentari in materia di amministratori di Sistema, la Società si impegna a collaborare, nei limiti delle proprie competenze tecniche/organizzative e delle proprie risorse, con il Titolare affinché siano sviluppate, adottate ed implementate misure correttive di adeguamento ai nuovi requisiti.

Articolo 8

Violazione dei Dati personali

1. LAZIOCrea è tenuta ad informare di ogni violazione di dati personali (cd. data breach) la Regione Lazio ed il Data Protection Officer, tempestivamente e senza ingiustificato ritardo, al fine di rispettare i termini di cui all'articolo 33 GDPR. Tale notifica – da effettuarsi tramite PEC alle Direzioni regionali competenti in materia per i servizi affidati attraverso il POA e contestualmente al DPO della Regione Lazio - deve essere accompagnata da ogni documentazione utile, ai sensi degli artt. 33 e 34 del GDPR, per permettere al Titolare, ove ritenuto necessario, di notificare la violazione all'Autorità Garante per la protezione dei dati personali e/o darne comunicazione agli interessati, entro il termine di 72 ore da quando il Titolare ne è venuto a conoscenza. Nel caso in cui il Titolare debba fornire informazioni aggiuntive alla suddetta Autorità Garante, LAZIOCrea supporterà il Titolare nella misura in cui le informazioni richieste e/o necessarie per l'Autorità Garante siano esclusivamente in possesso del Responsabile e/o di suoi ulteriori Responsabili.

Articolo 9

Nomina di ulteriori responsabili (sub-Responsabili)

1. In esecuzione e nell'ambito dei Servizi, LAZIOCrea, ai sensi dell'art. 28 comma 2 del GDPR, è autorizzata, salva diversa comunicazione scritta del Titolare, a ricorrere alla nomina di Ulteriori Responsabili, previo esperimento delle necessarie procedure di selezione degli operatori economici applicabili di volta in volta.
2. LAZIOCrea è tenuta, in sede di individuazione degli eventuali Ulteriori Responsabili e/o della loro sostituzione, ad informare preventivamente la Regione Lazio, al fine di consentire a quest'ultima, in attuazione dell'art. 28 comma 2 summenzionato, di poter manifestare eventuale formale opposizione alla nomina entro e non oltre il congruo termine di 20 (venti) giorni dalla ricezione della comunicazione. Decorso detto termine, LAZIOCrea potrà procedere all'effettuazione delle nomine, normativamente previste, nei confronti degli Ulteriori Responsabili individuati.
3. La nomina di Ulteriori responsabili da parte di LAZIOCrea sarà possibile a condizione che sull'Ulteriore Responsabile siano imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti richiesti dalla Normativa Privacy, salvo le ulteriori e più dettagliate istruzioni specifiche in riferimento alla particolare tipologia del servizio affidato che le Direzioni competenti per materia riterranno di dover adottare.
4. Qualora gli Ulteriori responsabili omettano di adempiere ai propri obblighi in materia di protezione dei dati, LAZIOCrea conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'Ulteriore Responsabile.
5. LAZIOCrea, infine, si obbliga a comunicare al Titolare, con cadenza annuale, eventuali modifiche ed aggiornamenti dei trattamenti di competenza dei propri Ulteriori Responsabili.

Articolo 10

Vigilanza, sanzioni e responsabilità

1. Ai sensi e per gli effetti dall'art. 28, comma 3 del GDPR, al fine di vigilare sulla puntuale osservanza della legge applicabile e delle istruzioni impartite a LAZIOCrea, il Titolare, anche tramite il proprio Responsabile della Protezione Dati e/o altro soggetto allo scopo individuato, potrà effettuare periodiche azioni di verifica. Tali verifiche, che potranno anche comportare l'accesso a locali o macchine e programmi del Responsabile, potranno aver luogo a seguito di comunicazione da parte del Titolare, da inviare con un preavviso di almeno cinque giorni lavorativi. Nell'ambito di tali verifiche, il Responsabile fornirà l'assistenza ed il supporto necessario, rispondendo alle richieste del Titolare, in relazione ai dati e ai trattamenti rispetto ai quali ha valore il presente atto di nomina.
2. Le Parti del presente Atto sono soggette, a cura dell'Autorità di controllo, alle sanzioni pecuniarie ai sensi dell'art. 83 del GDPR. Ferma restando l'applicazione di tale norma e, in generale, della Normativa Privacy, il mancato rispetto delle funzioni delegate e delle istruzioni impartite al Responsabile ovvero la violazione delle condizioni prescritte, darà luogo - anche in relazione a quanto previsto dal Contratto quadro di servizio - all'applicazione di penali e/o alla risoluzione del Contratto.
3. Il Responsabile ha la piena responsabilità diretta verso gli Interessati per i danni subiti derivanti da inadempimento o da violazione delle istruzioni legittime del Titolare con riferimento ai servizi affidati attraverso il POA.
4. LAZIOCrea, si obbliga a manlevare il Titolare e tenere quest'ultimo indenne da qualsiasi tipo di conseguenza, sia civile che amministrativa, responsabilità, perdita, onere, spesa, danno o costo da quest'ultimo sopportato per comportamenti attribuibili al Responsabile, ovvero di violazioni agli obblighi o adempimenti prescritti dalla Normativa Privacy ovvero di inadempimento delle pattuizioni contenute nel presente Atto, ovvero dei compiti assegnati dal Titolare.