POLICY PRIVACY
REGOLAMENTO UE 679/2016

SOMMARIO

POLICY PRIVACY LAZIOCREA SPA

1. PREMESSA

Il presente documento stabilisce le regole e le norme di comportamento adottate da LAZIOcrea SpA in ordine alle operazioni di trattamento dei dati effettuate dal personale dipendente della società stessa nel perseguimento della propria mission aziendale nonché descrive le misure di sicurezza e gli adempimenti effettuati in osservanza del Regolamento Unione Europea 679/2016.

L'insieme delle regole, norme, misure di sicurezza e adempimenti normativi sopra menzionati compone la presente Policy Privacy di LAZIOcrea al cui rispetto sono tenuti tutti coloro che agiscono in nome e per conto della stessa (il personale dipendente, il management e gli stakeholders).

Il presente documento relativo alla Policy Privacy è pubblicato sia sul sito internet che intranet aziendale, nelle apposite sezioni dedicate alla Privacy.

1.1 Definizioni

Art.4

Si riportano di seguito le definizioni normative di cui all'art. 4 del Regolamento UE 679/2016.

1) **«dato personale»:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) **«trattamento»:** 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, raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) **«limitazione** di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «titolare del trattamento»: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta 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;

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale d un persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'artico- regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:
a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

2 QUADRO NORMATIVO

2.1 Introduzione

Dopo un iter legislativo durato quattro anni, il 24 Maggio 2016 è entrato in vigore nel nostro ordinamento il Regolamento Europeo sulla Privacy 2016/679 (in avanti GDPR acronimo di General data protection regulation) che sostituisce il previgente Codice della Privacy (D.Lgs 196/2003) e al quale tutte le Pubbliche Amministrazioni e le società pubbliche e private dovranno conformarsi entro il 25 Maggio 2018. Oltre a introdurre nuovi istituti in materia di protezione dei dati personali e a rimodulare quelli già previsti dalle normative nazionali, il menzionato Regolamento segna un innalzamento qualitativo e quantitativo della disciplina del settore, collocandola in una dimensione necessariamente transfrontaliera poiché, nella società attuale, la privacy non può più essere considerata solo un fenomeno giuridico ma anche economico, e dettarne una regolamentazione condivisa a livello europeo risultava essenziale per dare ordine all'economia digitale finora dominata dai colossi statunitensi del web.

(Nota: le stime della Commissione UE hanno valutato che un mercato unico digitale pienamente funzionante potrà apportare fino a 415 miliardi di euro all'anno all'economia dell'area euro)

Per raggiungere questo obiettivo, la nuova normativa europea impone ai soggetti destinatari numerosi ed impegnativi adempimenti e obblighi ai quali conformarsi entro il termine sopra indicato. In particolare, come meglio specificato nei paragrafi successivi, i vigenti parametri normativi impongono di procedere ad una complessiva analisi e/o riorganizzazione dei processi, alla riprogettazione/rivisitazione dell'intero sistema informativo (gestione dei flussi informativi

interni ed esterni, progettazione ed implementazione delle misure di sicurezza tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio) e alla revisione di tutti i contratti, deleghe e nomine precedentemente effettuati.
Per ulteriori approfondimenti circa gli obblighi, le prescrizioni e le sanzioni previste dalla vigente normativa europea si rinvia a quanto specificato di seguito e/o al testo normativo del Regolamento in questione.

2.2 Principi contemplati dal Regolamento UE sulla Privacy (GDPR)

Il Regolamento Europeo sulla Privacy - dall'art. 5 all'art. 11 - contempla una serie di principi a cui il Titolare del Trattamento (e/o il Responsabile del trattamento limitatamente alla tipologia di attività effettuate) deve attenersi nelle operazioni di trattamento dei dati personali.

Si elencano di seguito i menzionati principi nonché la portata normativa degli stessi.

- Liceità: il trattamento dei dati personali deve essere effettuato nel rispetto delle norme di legge (non solo della normativa in materia di Privacy).
- Correttezza: il trattamento dei dati personali deve essere effettuato nel rispetto delle esigenze reciproche del Titolare e dell'interessato al trattamento.
- Trasparenza: Il Titolare deve assicurare la consapevolezza dell'interessato in ordine al trattamento dei suoi dati.
- Limitazione delle finalità: il trattamento dei dati personali deve essere effettuato per scopi (finalità) determinati, espliciti e legittimi; trattamenti successivi a quelli iniziali (ovvero a quelli per cui i dati sono stati inizialmente raccolti) non devono avere finalità incompatibili a quella originale (salvo casi espressamente previsti dalla legge come ad esempio ulteriori trattamenti per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche).
- Minimizzazione dei dati: il trattamento dei dati personali deve essere adeguato, pertinente e limitato a quanto necessario per il perseguimento delle finalità per le quali i dati stessi sono stati raccolti.
- Esattezza: i dati trattati devono essere esatti e, se necessario, aggiornati; il Titolare del trattamento deve adottare tutte le misure ragionevoli e necessarie al fine di cancellare e/o rettificare tempestivamente i dati inesatti.
- Limitazione della conservazione: i dati trattati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati stessi sono stati trattati (salvo trattamenti di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche.
- Integrità e riservatezza: I dati devono essere trattati in modo da garantire un'adeguata sicurezza e protezione dei dati stessi, mediante misure tecniche e organizzative adeguate e idonee ad evitare trattamenti non autorizzati e/o illeciti, perdita e/o distruzione dei dati trattati e/o danni accidentali.

2.3 Diritti degli Interessati contemplati dal Regolamento Europeo sulla Privacy

Il Regolamento Europeo sulla Privacy - dall'art. 12 all'art. 23 – assegna all'interessato del trattamento (salvo eccezioni stabilite dall'art. 23) tutta una serie di diritti a cui corrispondono obblighi da parte del Titolare del Trattamento.
Si riporta di seguito un elenco dei menzionati diritti riconosciuti dalla normativa europea agli interessati (ossia persone fisiche a cui si riferiscono i dati trattati).

- *Diritto all'Informativa*

Sia il riconoscimento del diritto all'informativa che il contenuto della stessa ricalca sostanzialmente quanto già previsto dalla disciplina nazionale sulla Privacy di cui al D.Lgs 196/2003. Tuttavia il Regolamento Europeo introduce due elementi di novità. Il primo consiste nella distinzione tra i trattamenti dei dati raccolti presso l'interessato (art. 13) e quelli raccolti presso un soggetto diverso (art. 14). Il secondo consiste nell'indicazione dei termini di cancellazione dei dati
Si elencano i contenuti principali dell'informativa prescritta dal R. UE

Art. 13

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati persona-li sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per tale periodo;

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'art. 6, paragrafo 1 lettera a) oppure sull'art. 9 paragrafo 2 lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

e) se la comunicazione dei dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

f) esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore tratta-mento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Art 14

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni;

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante.

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) le categorie di dati personali in questione;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

a) Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1 lettera a), oppure sull'articolo 9, paragrafo 2 lettera a) l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

e) il diritto di proporre reclamo a un'autorità di controllo;

f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all' articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:

a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;

b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la comunicazione dei dati personali;

4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.

5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo proporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure

d) qualora i dati personali debbono rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

- *Diritto di Accesso*

L'interessato al trattamento ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi e a tutta una serie di informazioni specificatamente elencate dall'art. 15 del GDPR (es. finalità del trattamento, categorie di dati trattati, destinatari a cui i dati vengono comunicati, etc.)

- *Diritto di rettifica*

L'interessato al trattamento ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Inoltre, tenuto conto delle finalità del trattamento, l'interessato stesso ha il diritto di ottenere l'integrazione dei propri personali incompleti.

- *Diritto alla cancellazione (diritto all'oblio)*

L'interessato al trattamento ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare ha l'obbligo di cancellare gli stessi se ricorrono i motivi specificatamente previsti dall'art. 17, paragrafo 1, del GDPR (es. i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti, l'interessato revoca il consenso, i dati sono trattati illecitamente, etc). Tuttavia La norma prevede delle eccezioni nei casi tassativamente elencati (es adempimento di un obbligo di legge, esecuzione di compiti svolti nel pubblico interesse o nell'esercizio di pubblici poteri, per motivi di archiviazione nel pubblico interesse o per fini di ricerca scientifica e storica, fini statistici, etc).
Il successivo paragrafo 2 art. 17 prescrive (Diritto all'Oblio) che. nel caso in cui il Titolare abbia reso pubblici i dati personali (es. adempimento obblighi di legge o esercizio del diritto all'informazione e/o di cronaca) è obbligato a cancellare i dati - tenendo conto della tecnologia disponibile e dei costi di attuazione- e di adottare le misure ragionevoli, anche tecniche, al fine di informare altri Titolari e/o Responsabili che stanno trattando i dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati.
Al riguardo risulta importante evidenziare che il riconoscimento del diritto all'oblio costituisce una novità introdotta dal R. UE. intesa come diritto di un individuo ad essere dimenticato o non essere più ricordato per fatti che lo riguardano e che in passato sono stati oggetto di cronaca

- *Diritto di limitazione del trattamento*

Altra novità introdotta dal GDPR è il riconoscimento del diritto dell'interessato di ottenere dal Titolare la limitazione del trattamento dei dati che lo riguardano nelle ipotesi tassativamente previste dall'art. 18 del Regolamento stesso (es. se l'interessato ha contestato l'esattezza dei dati, se il trattamento è illecito, l'interessato si è opposto al trattamento, etc.)

(Nota: in riferimento ai sopra menzionati diritti il titolare ha l'obbligo non solo di ottemperare alle relative prescrizioni ma ha altresì l'obbligo di comunicare a ciascun destinatario cui sono sono stati trasmessi i dati personali, le eventuali rettifiche o cancellazioni o limitazioni del trattamento richieste dall'interessato, salvo che ciò non si rilevi impossibile o implichi uno sforzo sproporzionato).

- *Diritto alla Portabilità dei dati*

Altra novità introdotta dal GDPR è il riconoscimento del diritto dell'interessato al trattamento di ricevere dal Titolare del trattamento tutti i dati personali che lo riguardano in un formato strutturato, di uso comune e leggibile da dispositivo automatico e interoperabile, in modo che l'interessato possa trasmettere agevolmente i propri dati ad altro Titolare come stabilito dall'art. 20 R.E.
In proposito risulta importante evidenziare che il riconoscimento del citato diritto costituisce una novità introdotta dal R.E. finalizzata a rafforzare ulteriormente il controllo da parte dell'interessato sui propri dati personali trattati con mezzi automatizzati.

- *Diritto di Opposizione*

L'interessato al trattamento ha il diritto di opporsi in qualsiasi momento al trattamento dei dati che lo riguardano se ricorrono le ipotesi elencate dall'art. 21 GDPR (compresa la profilazione).

Anche in questo caso la norma prevede delle eccezioni (es. per l'esercizio e/o l'accertamento e/o la difesa di un diritto in sede giudiziaria, per finalità di marketing, etc

- *Diritto di non essere sottoposto a processi decisionali automatizzati, compresa la profilazione.*

Altra novità introdotta dal GDPR. è il riconoscimento del diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o comunque che incida significativamente sulla persona. Tuttavia, anche in questo caso, la norma (art 22 R.E.) prevede delle eccezioni tassativamente previste (ad es consenso esplicito dell'interessato, se il citato trattamento risulta necessario ai fini della conclusione e/o esecuzione di un contratto, ai fini della tutela di un diritto, interesse legittimo, etc.)

2.4. Principio dall'Accountability e figure previste dal Regolamento Europeo

ART.24
Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento UE 679/2016. Dette misure sono riesaminate e aggiornate qualora necessario.

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 R. UE può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

In conclusione, il principio di responsabilizzazione (c.d Accountability) richiede al titolare del trattamento di mettere in atto misure di sicurezza adeguate per garantire, ed essere in grado di dimostrare, che i trattamenti effettuati dallo stesso siano conformi alle disposizioni normative di cui al R. UE.

ART.27
Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione.

1. Ove si applichi l'articolo 3, paragrafo 2, il titolare del trattamento o il responsabile del trattamento designa per iscritto un rappresentante nell'Unione.

2. L'obbligo di cui al paragrafo 1 del presente articolo non si applica:
   a) al trattamento se quest'ultimo è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativa a condanne penali e a reati di cui all'articolo 10, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento; oppure
   b) alle autorità pubbliche o agli organismi pubblici.

3. Il rappresentante è stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato.

4. Ai fini della conformità con il presente regolamento, il rappresentante è incaricato dal titolare del trattamento o dal responsabile del trattamento a fungere da interlocutore, in aggiunta o in sostituzione del titolare del trattamento o del responsabile del trattamento, in particolare delle autorità di controllo e degli interessati, per tutte le questioni riguardanti
il trattamento.

5. La designazione di un rappresentante a cura del titolare del trattamento o del responsabile del trattamento fa salve le azioni legali che potrebbero essere promosse contro lo stesso titolare del trattamento o responsabile del trattamento.

ART.28
Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere,

un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono 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 contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

ART.29
Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
In conclusione, il Regolamento UE 679/2016 – analogamente alla normativa nazionale di cui al D.Lgs 196/2003 – prevede la figura del Responsabile del trattamento (art. 4 paragrafo 8 - definizioni) ossia la persona fisica o giuridica (in certi casi anche un'autorità pubblica, il servizio o altro organismo) che tratta dati per conto del Titolare del trattamento.
Novità introdotta dal Regolamento è la possibilità per il Responsabile di nominare altro Responsabile (sub-responsabile) previa autorizzazione del Titolare. Il primo Responsabile risponde degli inadempimenti del secondo Responsabile.
Da ultimo si specifica che il Regolamento, pur non prevedendo specificatamente la figura degli incaricati del trattamento (prevista invece dall'art. 30 del D.Lgs 196/2003), contempla le figure degli autorizzati al trattamento (figure comunque riconducibili alla figura degli incaricati prevista dalla normativa nazionale sulla privacy). In particolare il combinato disposto degli articoli 4, paragraf. 10 e art. 29 introducono le figure dei soggetti autorizzati al trattamento dei dati personali sotto l'autorità diretta del Titolare e/o del Responsabile, i quali devono essere istruiti in tal senso.

2.5 Il responsabile della protezione dei dati

Principale novità prevista dal Regolamento Europeo sulla Privacy risulta essere l'obbligo del Titolare (e/o del Responsabile) del Trattamento di nominare un Responsabile della protezione dei dati (c.d. data protection officer o DPO), ovvero un professionista che possieda un'adeguata conoscenza della normativa e della prassi di gestione dei dati personali, che sia in grado di adempiere alle proprie funzioni in piena indipendenza e in assenza di conflitti di interesse, operando come dipendente o sulla base di un contratto di servizio.

In proposito risulta importante evidenziare che il Responsabile della protezione dei dati deve essere designato in funzione delle qualità professionali – ovvero conoscenza specialistica della normativa e della prassi in materia di protezione dei dati come disposto dall'art. 37 paragrafo 5 del GDPR - e della capacità di assolvere i compiti attribuiti dal successivo art. 39, ovvero in estrema sintesi: verificare che la normativa vigente e le policy interne del Titolare (e/o Responsabile) siano correttamente attuate e applicate, incluse le attribuzioni delle responsabilità e i relativi controlli/audit, informare e fornire consulenza in merito agli obblighi derivanti dalla normativa stessa, fungere da punto di contatto per l'Autorità di Controllo (Garante della Privacy) per tutte le questioni connesse al trattamento dei dati e per i procedimenti di consultazione previsti dalla legge, cooperando con la stessa in ordine alla corretta attuazione della normativa in questione.

(Nota: come prescritto dal R. UE., gli estremi identificativi del Responsabile della Protezione dei Dati personali devono essere pubblicati e comunicati all'Autorità Nazionale di Controllo ossia al Garante della Privacy)

2.6 Privacy by Design - Privacy by default

Atteso l'obbligo gravante sul Titolare e sul Responsabile di adottare le misure di sicurezza (come meglio specificato di seguito), si evidenzia che la fase di progettazione delle stesse (misure sia tecniche che organizzative) dovrà avvenire nel rispetto dei requisiti previsti dal Regolamento Europeo di Privacy by design (che impone di progettare sistemi e applicativi sul principio dell'uso minimo e indispensabile dei dati personali) e Privacy by default (che impone di progettare misure e sistemi che abbiano come impostazione predefinita solo l'uso dei soli dati necessari per una specifica finalità) .

In particolare l'art. 25 GDPR (privacy by design) rubricato "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita"* prescrive che: al par. 1) "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati".

Al Par. 2) (privacy by default) "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In

particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica". Par 3): "Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo").

In conclusione Il Titolare (e/o i Responsabile) del trattamento sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso deve mettere in atto misure tecniche ed organizzative adeguate – quali ad es. la pseudonimizzazione – volte a ridurre al minimo il trattamento dei dati personali e, quindi, ad attuare in modo efficace i principi di protezione dei dati e le garanzie contemplate dal R.E.

(Nota: In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni devono tener conto del diritto alla protezione dei dati, in modo da assicurarsi che i Titolari e/Responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati personali. Dunque il principio della protezione dei dati fin dalla progettazione deve essere preso in considerazione anche nell'ambito delle procedure di appalto).

2.7 Registro dei trattamenti

Altro obbligo - prescritto dall'art. 30 GDPR - a carico sia del Titolare che del Responsabile del Trattamento è la tenuta di un **registro delle attività di trattamento** svolte sotto le rispettive responsabilità.

I menzionati registri (un registro del Titolare e uno del Responsabile, quest'ultimo deve riguardare le attività di trattamento svolte per conto del titolare), da tenere in forma scritta (anche in formato elettronico), devono essere messi a disposizione dell'Autorità Garante per ispezioni e controlli.

Si elencano di seguito le informazioni principali che devono contenere i registri in questione.

- ✓ Nome e dati di contatto del Titolare e/o del Responsabile del trattamento e del responsabile della protezione dei dati.
- ✓ Le finalità del trattamento.
- ✓ Una descrizione della categoria di interessati e della categoria di dati personali.
- ✓ Le categorie di destinatari a cui i dati personali sono stati o saranno comunicati.
- ✓ Se possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati (obbligo solo per i Titolari).
- ✓ Se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Per ulteriori approfondimenti si rinvia all'art. 30 del R.E.

2.8. Sicurezza dei dati e valutazione dei rischi (art. 32 Regolamento UE)

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento (e/o il Responsabile del Trattamento limitatamente all'ambito e alla tipologia dei trattamenti effettuati) ha l'obbligo – prescritto dall'art. 32 del Regolamento Europeo

- di mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al regolamento stesso.
Pertanto, il menzionato regolamento prevede l'attuazione di politiche adeguate in materia di protezione dei dati personali, incentrate principalmente sull'obbligo da parte dei Titolari del trattamento (e/o Responsabili) di adottare misure di sicurezza idonee (a garantire un livello di sicurezza adeguato al rischio) sulla base di una previa valutazione dei rischi secondo il principio di responsabilizzazione (ovvero il principio secondo cui risulta necessario garantire, ed essere in grado di dimostrare, la conformità dei trattamenti effettuati sui dati alla normativa vigente).

2.9. Sicurezza dei dati, valutazione di impatto e consultazione preventiva (art. 35 Regolamento UE)

Come detto sopra il Regolamento Europeo sulla Privacy prevede l'obbligo da parte del Titolare del Trattamento (e/o del Responsabile del Trattamento in riferimento alla tipologia di trattamenti effettuata) di adottare misure di sicurezza, tecniche ed organizzative, idonee a garantire un adeguato livello di sicurezza e di protezione dei dati personali trattati. In particolare il citato Regolamento non prevede un elenco di misure di sicurezza, ma impone l'obbligo di adottare le stesse sulla base di una preventiva valutazione dei rischi che tenga conto delle eventualità di distruzione accidentale o illegale dei dati trattati, perdita, modifica, rivelazione o accesso non autorizzato ai dati trasmessi, conservati o comunque trattati. Laddove i trattamenti effettuati presentino un rischio elevato per i diritti e le libertà delle persone, il Titolare del Trattamento ha l'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati per determinare l'origine, le natura e la gravità di tale rischio.
Tuttavia se la tecnologia disponibile o i costi di attuazione non rendono possibile l'adozione di misure di gestione del rischio elevato, prima di effettuare le operazioni di trattamento sui dati a rischio elevato, il Titolare deve consultare l'Autorità di controllo c.d. **procedimento di consultazione preventiva.**

(Nota: al riguardo si precisa che la valutazione dei rischi e la valutazione di impatto sono due istituti giuridici diversi. In particolare la valutazione dei rischi deve essere sempre effettuata (ed infatti è un onere sia a carico del Titolare che del Responsabile del trattamento) al fine di individuare le misure di sicurezza da adottare a presidio dei rischi esistenti (e/o adeguare le misure di sicurezza adottate). La valutazione di impatto (c.d. DPIA), invece, è un'attività che deve essere effettuata solo su quei trattamenti che presentano un rischio elevato per i diritti e le libertà fondamentali (è un onere a carico solo del Titolare).

2.10. Data Breach

Il regolamento Europeo prevede l'obbligo del Titolare del Trattamento di notificare all'Autorità di controllo la violazione dei dati personali (**Data Breach**) senza ingiustificato ritardo (ove possibile entro 72 ore dal momento in cui il Titolare stesso sia venuto a conoscenza di tale violazione). Laddove la citata violazione venga riscontrata dal Responsabile del trattamento, lo stesso ha l'obbligo di informare il Titolare senza ingiustificato ritardo. Il R.E prescrive, inoltre, l'obbligo di comunicare la suindicata violazione all'interessato nel caso la stessa presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

2.11. Obbligo di formazione

Art. 29 Regolamento UE

Atteso l'obbligo di istruire coloro che trattano i dati personali sotto la diretta autorità del Titolare e/o Responsabile del trattamento prescritto dal suindicato art. 29, si evince l'obbligo per il Titolare/Responsabile stesso di formare coloro (il personale dipendente, ivi compresi i soggetti con funzioni direttive/dirigenziali) tratta i dati personali differenziato a seconda delle tipologie di attività svolte e/o particolari funzioni tecniche assegnate e/o particolari incarichi/responsabilità conferiti).

2.12. Codici di condotta e certificazioni

Altra novità introdotta dal GDPR è l'obbligo da parte delle Autorità di Controllo di incoraggiare i Titolari (e/o i Responsabili) del trattamento ad aderire ai codici di condotta e a meccanismi di certificazione. In particolare, in base al disposto normativo, l'adesione ai predetti codici e la certificazione risultano essere attività volontarie e non obbligatorie; tuttavia possono essere utilizzate come strumento per dimostrare la conformità dei trattamenti effettuati alla normativa europea, ossia sono uno strumento per Titolari e/o Responsabili volto a documentare il rispetto degli obblighi e delle prescrizioni ivi contemplati.

(Nota: le associazioni e gli organismi rappresentanti le categorie dei Titolari e/o Responsabili del Trattamento possono elaborare codici di condotta allo scopo di precisare l'applicazione del R.E. Quindi i Titolari e/o Responsabili del Trattamento vi possono aderire e/o comunque adottare propri codici di condotta in linea con quelli adottati dai rispettivi rappresentanti)

2.13 Impianto Sanzionatorio (articoli 77 e ss)

Il Regolamento UE prevede due forme di tutela dell'interessato (ossia soggetto a cui si riferiscono i dati trattati): amministrativa e giurisdizionale.

Tutela giurisdizionale: l'interessato ha il diritto di proporre un ricorso davanti le autorità giurisdizionali competenti per la tutela dei propri diritti.
Inoltre si specifica che:
Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento UE ha il diritto di ottenere il risarcimento del danno dal Titolare e/o dal Responsabile del trattamento. La relativa azione legale deve essere promossa dinanzi alle autorità giurisdizionali competenti a norma del diritto della Stato Membro.
Il Responsabile del trattamento risponde del danno causato dal trattamento solo se non ha adempiuto agli obblighi del Regolamento UE specificatamente diretti ai Responsabili del trattamento o se ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento.
In caso più Titolari e/o Responsabili del trattamento siano responsabili del danno causato, il Regolamento UE prevede la responsabilità in solido per l'intero ammontare del danno stesso, prevedendo altresì il diritto di rivalsa di chi abbia pagato l'intero importo.
Il Titolare o il Responsabili del trattamento è esonerato da responsabilità, se dimostra che l'evento dannoso non gli è in alcun modo imputabile (si applica la cosiddetta inversione dell'onere della prova).

Tutela amministrativa: l'interessato, se ritiene di essere stato leso nelle sue prerogative, ha diritto di proporre reclamo all'autorità di controllo (Garante per la protezione dei dati personali), fatto salvo ogni altro ricorso amministrativo o giurisdizionale.

Criteri di applicazione delle Sanzioni amministrative.
L'art. 83 del Regolamento UE rubricato "*Condizioni generali per infliggere sanzioni amministrative pecuniarie*" prevede che ogni autorità di controllo provvede affinchè le sanzioni amministrative pecuniarie inflitte siano in ogni caso effettive, proporzionate e dissuasive.
Tali Sanzioni sono inflitte in funzione di ogni singolo caso e nel fissarne l'ammontare si tiene conto degli elementi previsti dall'art. 83 paragrafo 2 (es: natura, gravità e durata della violazione; numero di interessati lesi e livello del danno causato; carattere doloso o colposo della violazione; misure adottate dal Titolare e/o Responsabile del trattamento per attenuare il danno subito dagli interessati; grado di responsabilità di questi ultimi ed eventuali precedenti violazioni commesse; grado di cooperazione con l'autorità di controllo; categorie di dati personali interessate dalla violazione; adesione ad eventuali codici di condotta e/o meccanismi di certificazione; e, più in generale, qualsiasi altro fattore aggravante o attenuante applicabile alle circostanze del caso)
A seconda delle disposizioni normative violate sono previste sanzioni fino a 10.000.000,00 euro (o per le imprese fino al 2% del fatturato annuo dell'esercizio precedente se superiore) o fino a 20.000.000,00 euro (o per le imprese fino al 4% del fatturato annuo dell'esercizio precedente se superiore).
In caso di violazione di più disposizioni normative l'importo totale della sanzione pecuniaria non supera l'importo specificato per la violazione più grave.
Da ultimo si rileva che le sanzioni pecuniarie possono essere inflitte dall'autorità di controllo in aggiunta alle misure previste dall'art. 58 Regolamento UE (provvedimenti di ingiunzione, di accesso ai dati e/o ai locali del Titolare/Responsabile, di ammonizione, ordinatori, di revoca, di autorizzazione, etc.)

3 ATTRIBUZIONE DI RESPONSABILITA' E CONFERIMENTO DI INCARICHI AL MANAGEMENT ED AL PERSONALE DIPENDENTE LAZIOCREA SPA

Prima di rappresentare le attività effettuate in materia di attribuzione di responsabilità e conferimento di incarichi al personale dipendente e al management di LAZIOcrea, risulta opportuno evidenziare le modalità utilizzate in osservanza dei parametri normativi stabiliti. Nel dettaglio si è tenuto conto dei seguenti fattori:

- Il contesto operativo ed organizzativo dell'azienda ovvero da una parte le deleghe di funzione e le responsabilità attribuite al management (organigramma aziendale) e dall'altra gli incarichi e le diverse tipologie di attività lavorative assegnate al personale dipendente (microstruttura aziendale).
- Il diverso regime giuridico sotteso alle operazioni di trattamento dei dati effettuate dal personale dipendente e dal management di LAZIOcrea. In particolare sono stati considerati da una parte i trattamenti di dati rientranti nella sfera di titolarità della LAZIOcrea ai sensi dell'art. 4, paragrafo 7, del Regolamento UE (ovvero i dati afferenti a tutto il personale dipendente, compresi consulenti, collaboratori e fornitori) e dall'altra i trattamenti di dati

rientranti nella sfera di titolarità della Regione Lazio e degli Enti alla stessa collegati (ovvero i dati afferenti agli utenti/cittadini dell'amministrazione regionale e delle strutture pubbliche collegate) ai sensi del medesimo articolo in virtù dei quali LAZIOcrea è Responsabile del trattamento ai sensi del successivo paragrafo 8.

(Nota; i servizi svolti da LAZIOcrea a supporto della Regione Lazio - Progetti/Servizi contemplati dal contratto quadro e dettagliati nel POA - implicano continui trattamenti di dati personali per conto della stessa e degli Enti collegati)

- La natura e le diverse tipologie di attività effettuate (analisi dei processi) al fine di individuare l'ambito del trattamento consentito al personale incaricato/autorizzato al trattamento.
- Le modalità con cui sono effettuate le operazioni di trattamento, ossia con supporti cartacei e/o con strumenti informatici, con particolare riferimento agli applicativi informatici e/o banche dati utilizzate.

Tanto premesso, LAZIOcrea ha provveduto alla designazione – con atto scritto - di tutto il personale dipendente (ivi compreso il management) ad "*incaricato del trattamento dei dati personali*" ovvero ha autorizzato lo stesso all'effettuazione delle operazioni di trattamento fornendo le relative istruzioni in linea con i parametri normativi previsti dal Regolamento UE (art. 29).

I predetti atti di nomina sono continuamente aggiornati in linea con le modifiche dell'assetto organizzativo aziendale nonché con i cambiamenti delle attività lavorative svolte dal personale (es. mobilità, conferimento di nuovi incarichi, etc.).

Inoltre LAZIOcrea ha provveduto a designare il Responsabile della protezione dei dati personali (Data protection officer o D.P.O) ai sensi dell'art. 37 GDPR. con deliberazione del Consiglio di Amministrazione del 22.05.2016.

(Nota: il DPO figura centrale prevista dalla normativa europea a garanzia della corretta attuazione della stessa da parte delle P.A. e di imprese pubbliche e private nonché interfaccia tra queste ultime e l'autorità nazionale di controllo/Garante Privacy).

4 ADEMPIMENTI EFFETTUATI E MISURE DI SICUREZZA ADOTTATE DA LAZIOCREA SPA IN OSSERVANZA DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI DI CUI AL REGOLAMENTO U.E 679/2016

4.1 Predisposizione dei registri delle attività di trattamento in osservanza dell'art. 30 R.E.

Atteso l'obbligo per i Titolari e/o i Responsabili del trattamento di redigere un registro dei trattamenti da mettere a disposizione del Garante Privacy in caso di ispezioni/controlli in osservanza del suindicato art 30, LAZIOcrea ha provveduto ad effettuare le relative attività come specificato di seguito.

In particolare, considerato il diverso regime giuridico sotteso alle categorie di dati trattati da LAZIOcrea (dati rientranti nella sfera di titolarità della società stessa e dati rientranti nella sfera di titolarità della Regione Lazio), devono essere redatti due Registri:

- ✓ il primo Registro in osservanza del relativo obbligo a carico del Titolare del trattamento; dunque LAZIOcrea dovrà mappare tutte le operazioni di trattamento dei dati personali

rientranti nella sfera di Titolarità dell'azienda stessa (ossia i dati afferenti al personale dipendente, ai collaboratori, ai consulenti esterni, ai legali rappresentanti dei fornitori e/o Enti pubblici/privati convenzionati e/o che a vario titolo interagiscono con l'azienda)

- ✓ Il secondo Registro in osservanza del relativo obbligo a carico del Responsabile del trattamento; dunque LAZIOcrea – in qualità di Responsabile esterna del trattamento dei dati personali rientranti nella sfera di Titolarità della Regione Lazio e degli enti alla stessa collegati - dovrà mappare tutte le categorie di trattamento dei dati effettuate per conto di ogni Titolare del trattamento (ossia Regione Lazio, ASL, Aziende Ospedaliere, Agenzie come ARES, AGEA, etc.)

(Nota: i dati personali trattati da LAZIOcrea per conto dell'amministrazione regionale (ivi comprese USL e AO) nell'ambito dei servizi/progetti dettagliati nel POA, sono quelli afferenti ai cittadini, utenti, personale dipendente dell'amministrazione stessa).

Premesso quanto sopra, è stato predisposto un documento (excel) denominato "Registro dei trattamenti/VIP" inviato a tutte le strutture aziendali che hanno proceduto alla relativa compilazione. Al riguardo si specifica che il citato documento, oltre a contenere le informazioni richieste dall'art. 30 (in ordine all'obbligo di tenuta dei Registri), contiene – in una scheda distinta – le informazioni inerenti ad una prima valutazione dei rischi sui trattamenti effettuati dalle diverse strutture aziendali che hanno provveduto alla relativa compilazione.

4.2 Revisione /predisposizione della parte documentale in materia di privacy.

LAZIOcrea ha provveduto ad una complessiva revisione/aggiornamento di tutta la documentazione, le informative e i regolamenti predisposti in materia di privacy in linea sia con i vigenti parametri normativi europei. In particolare sono state aggiornate tutte le informative pubblicate sui siti aziendali secondo i nuovi parametri normativi di cui agli articoli 13 e 14 del GDPR, è stato predisposto il presente documento denominato "policy privacy" aziendale (in sostituzione del Sistema Privacy precedentemente adottato in linea con la normativa nazionale sulla Privacy) e, da ultimo, è stato pubblicato un modulo relativo all'esercizio dei diritti degli interessati al trattamento (sopra elencati) previsto dalla normativa europea sulla Privacy.
In riferimento ai Regolamenti/procedure adottate in materia di sicurezza, utilizzo di strumenti informatici, posta elettronica, internet, etc. si rinvia ai relativi documenti pubblicati sui siti internet e intranet aziendali nelle apposite sezioni (MOG, Sistema Qualità, etc.)

4.3 Misure di Sicurezza

Come specificato sopra (quadro normativo), il Regolamento Europeo in materia di Privacy, non prevedendo un elenco specifico di misure di sicurezza, prescrive (art. 32) che le stesse debbano essere adottate sulla base di una valutazione dei rischi e, nei casi di riscontrato rischio elevato, sulla base di una valutazione di impatto sulla protezione dei dati (art 35).

Quindi, effettuate le attività di analisi di rischio aventi ad oggetto tutte le attività/servizi aziendali, si è provveduto ad effettuare l'adeguamento delle misure di sicurezza adottate ai nuovi parametri

normativi. Al riguardo risulta importante precisare che il predetto adeguamento è avvenuto nel rispetto dei requisiti previsti dal Regolamento Europeo di Privacy by design (che impone di progettare sistemi e applicativi sul principio dell'uso minimo e indispensabile dei dati personali) e Privacy by default (che impone di progettare misure e sistemi che abbiano come impostazione predefinita solo l'uso dei soli dati necessari per una specifica finalità).

(Nota: il GDPR sancisce l'obbligo, per i soggetti coinvolti nelle operazioni di trattamento di dati personali, di adottare le idonee e preventive misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento illecito e/o comunque non consentito o non conforme alle finalità della raccolta. La custodia, la sicurezza e il controllo dei dati personali deve essere adeguata alla natura dei dati stessi e alle specifiche caratteristiche del trattamento, nonché alle conoscenze acquisite in base al progresso tecnologico).

- *Misure di sicurezza adottate in relazione ai trattamenti con l'ausilio di strumenti elettronici*

In base a quanto stabilito dalla normativa in materia di Privacy – sia nazionale che europea - le operazioni di trattamento dei dati personali effettuate con strumenti elettronici/automatizzati, devono rispettare le misure di sicurezza adottate dal Titolare/Responsabile del trattamento specificate nei relativi regolamenti e/o procedure in materia di Privacy, in materia di utilizzo di strumenti informatici, internet e posta elettronica nonché in materia di sicurezza delle informazioni (ISO 27001).

In particolare si elencano di seguito le regole stabilite per l'utilizzo delle credenziali di autenticazione (password) assegnate al personale incaricato del trattamento (regole riportate negli atti di designazione degli incaricati – istruzioni operative) nonché i necessari accorgimenti/ cautele per assicurare la segretezza della componente riservata delle credenziali stesse e per la diligente custodia dei dispositivi elettronici (computer) in uso esclusivo e/o comunque in possesso dell'incaricato.

Nel dettaglio:

- Elaborare la password secondo le indicazioni fornite dal Titolare/Responsabile del trattamento e rispettare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (username).
- Elaborare la parola chiave in maniera che non contenga riferimenti agevolmente riconducibili all'incaricato (quindi, la parola chiave non dovrebbe essere: il nome o il cognome dell'incaricato, il soprannome, la data di nascita propria, dei figli o degli amici, il nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi, il nome e cognome di personaggi famosi, etc).
- Rispettare i profili di autorizzazione attribuiti dal Titolare/Responsabile ai fini dell'accesso ai dati e ai sistemi ovvero all'utilizzo di determinati applicativi informatici e/o piattaforme informatiche nell'ambito delle attività lavorative assegnate.
- Custodire in modo diligente i dispositivi elettronici in possesso e/o in uso esclusivo.
- Non rivelare la password (parola chiave) a terzi non autorizzati; non scrivere la password (parola chiave) in un messaggio di posta elettronica;
- Modificare la password (parola chiave) quando richiesto dal Sistema (i sistemi prevedono in automatico la modifica della parola chiave almeno ogni 6 mesi, in caso di trattamento di dati sensibili e/o giudiziari i sistemi prevedono detta modifica ogni tre mesi).

- Terminare la sessione di lavoro, al computer, ogni volta che l'incaricato si allontani, anche solo per poco tempo, dal proprio ufficio; in ogni caso deve essere attivata la funzione screen saver qualora l'incaricato si allontani, anche solo per pochi minuti, dal proprio ufficio.
- Mettere in atto gli accorgimenti ritenuti più opportuni affinché anche in sua assenza, il computer non resti incustodito e/o accessibile a terzi non autorizzati.
- Curare la conservazione e la segretezza della password (parola chiave) evitando di trascriverla su supporto cartaceo precario o visibile (es. post-it) oppure di tenerla nel portafoglio o trascritta nella prima pagina dell'agenda o della rubrica di ufficio o in qualunque altro posto facilmente intuibile;
- Al fine di tutelare l'integrità e la disponibilità dei dati trattati e memorizzati sui files di rete, utilizzare i sistemi di back up adottati dalla struttura amministrativa di riferimento secondo le istruzioni fornite dai responsabili della struttura stessa.

Inoltre, si specifica che:

- La password (parola chiave) prevista dal sistema di autenticazione è composta generalmente da almeno otto caratteri, di cui almeno quatto devono essere di natura numerica.
- Il codice per l'identificazione, laddove utilizzato, non e mai assegnato ad altri incaricati, neppure in tempi diversi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
- Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- Sono state adottate procedure di gestione delle credenziali di autenticazione e procedure per l'utilizzo del sistema di autorizzazione;
- Sono aggiornati periodicamente gli 'ambiti del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- Sono state adottate misure di protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, accessi non consentiti ai dati e/o a determinati programmi informatici;
- Sono state adottate procedure/regolamenti per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

(Nota: per strumenti elettronici il legislatore intende gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato.)

Nel dettaglio si elencano di seguito le principali misure di sicurezza adottate dall'Azienda e, come specificato sopra, riportate nei regolamenti e/o procedure aziendali pubblicati sui siti aziendali.

- Sistema di autenticazione informatica.

L'azienda ha adottato sistemi di autenticazione informatica ossia sistemi mediante i quali lo strumento elettronico è in grado di riconoscere l'identità dell'utente (può essere una password o un altro codice segreto).

(Nota. tutto il personale dipendente di LAZIOcrea risulta assegnatario di proprie credenziali di autenticazioni secondo la procedura di seguito indicata).

- Procedura di identificazione e di gestione delle credenziali di autenticazione e utilizzazione di un sistema di autorizzazione.

In conformità a quanto disposto dalla normativa in materia di Privacy, LAZIOcrea assicura che il trattamento dei dati personali, effettuato con strumenti elettronici, sia consentito in conformità al profilo di autorizzazione attribuito al personale incaricato dotato di una o più credenziali di autenticazione (ossia un codice per l'identificazione dell'incaricato associato a una parola chiave riservata e conosciuta solamente dal medesimo).

Pertanto, LAZIOcrea si è dotata di un Sistema di Autenticazione (user-id, password) e di un Sistema di Autorizzazione (ossia sono stati individuati profili di autorizzazione di ambito diverso individuati in relazione all'attività lavorativa effettuata) al fine di assicurare la riservatezza dei dati trattati. In proposito risulta importante evidenziare che specifiche istruzioni e indicazioni circa le modalità di gestione e utilizzo del sistema di autenticazione informatica e circa le regole sul rispetto dei profili di autorizzazione attribuiti (es. accesso a cartelle condivise solo per il personale che svolge le medesime attività lavorative), oltre ad essere elencate di seguito nel paragrafo denominato norme comportamentali, sono state riportate all'interno degli atti di nomina ad "incaricato del trattamento dei dati personali".

Inoltre LAZIOcrea ha adottato:

- ✓ un sistema di protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, accessi non consentiti a determinati programmi informatici. A titolo informativo e non esaustivo si riportano di seguito alcune misure di sicurezza:
    - Installazione - sui computer di proprietà di LAZIOcrea o in uso alla stessa – solo di software autorizzati (ovvero software valutati e adottati per i loro aspetti di funzionalità e sicurezza).
    - Controllo degli accessi fisici in Azienda;
    - Procedura inerente agli accessi ai sistemi informatici e alla gestione postazioni informatiche;

- ✓ Misure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi.

In proposito si precisa che l'Azienda, per gli elaboratori collegati in rete, ha provveduto ad assegnare un codice identificativo personale ad ogni Incaricato del Trattamento (che è unico e non può quindi essere assegnato a persone diverse). E' inoltre prevista la disattivazione di detti codici in caso di mancato utilizzo per un periodo di tempo superiore ai sei mesi. Tutti gli elaboratori collegati in rete sono muniti di software antivirus aggiornato. Per i server di rete sono previsti diversi sistemi di backup che assicurano il recupero dei dati in caso di malfunzionamento dei sistemi; inoltre per ogni server è previsto un ciclo di backup (le copie di backup sono custodite in osservanza delle misure di sicurezza previste dalla normativa in materia di Privacy).

- Sicurezza elettronica degli elaboratori in rete pubblica

La connessione di un PC aziendale ad una rete pubblica può avvenire solo previa autorizzazione formale in linea con le procedure adottate. Tali connessioni con l'esterno sono protette da adeguati sistemi software e/o hardware specifici disposti nei punti di interconnessione tra reti distinte (es tra una rete intranet e una rete internet) in grado di controllare automaticamente gli accessi alla rete ed eventualmente bloccare quelli non desiderati (il tutto in linea con i parametri di sicurezza adottati).

- Protezione locali server

I server di LAZIOcrea sono posizionati presso le strutture regionali (CED Regione Lazio) in locali adeguatamente protetti dove sono stati installati idonei controlli per permettere l'accesso solo al personale debitamente autorizzato. Per la sicurezza passiva sono installati dispositivi come rilevatori di fumo o calore, sirena di allarme antincendio, estintore, uscita di sicurezza. La protezione dei dati contenuti nei dispositivi di immagazzinamento dati dei server è garantita dal Responsabile della Direzione Sistemi Infrastrutturali.

- *Misure di Sicurezza in riferimento ai trattamenti effettuati senza l'ausilio di strumenti elettronici.*

In conformità a quanto disposto dalla Regolamento UE. 679/2016, LAZIOcrea SpA - in ordine alle operazioni di trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici (trattamenti cartacei) – ha adottato regole e misure minime di sicurezza riportate nei documenti pubblicati nonché negli atti di nomina del personale incaricato.
Si elencano di seguito le regole principali che il personale incaricato ha l'obbligo di rispettare nell'effettuazione delle operazioni di trattamento dei dati personali nonché le misure di sicurezza adottate dall'azienda.
Regole principali da osservare (riportate sia negli atti degli incaricati del trattamento che nel codice comportamentale – paragrafo successivo).

- I documenti che contengono dati personali non devono essere portati al di fuori dei locali, armadi e cassetti (protetti con serratura) individuati per la loro conservazione, se non in casi del tutto eccezionali e su autorizzazione del Titolare/Responsabile del trattamento anche per mezzo del Responsabile della struttura aziendale. L'eventuale asportazione deve essere ridotta al tempo minimo necessario per effettuare le necessarie operazioni di trattamento.
- Nel periodo di tempo in cui i documenti che contengono dati personali si trovano al di fuori dei locali, armadi e cassetti (protetti con serratura), individuati per la loro conservazione, l'incaricato del trattamento non deve lasciarli mai incustoditi. Al termine dell'orario di lavoro, l'incaricato stesso deve riportare tutti i documenti che contengono dati personali nei locali (archivi regionali), armadi e cassetti (protetti con serratura) individuati per la loro conservazione.
- I documenti (Faldoni, Raccoglitori, Fascicoli, etc.) che contengono dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro. Quindi risulta necessario adottare ogni cautela affinché persone non autorizzate non vengano a conoscenza dei dati personali e delle informazioni contenuti nei documenti utilizzati per lo svolgimento delle attività lavorative.
- Per evitare il rischio di divulgazione dei dati personali l'incaricato ha l'obbligo di limitare l'utilizzo di copie fotostatiche o di qualsiasi altra natura.
- L'azienda ha adottato regole che vietano di sottrarre, cancellare, distruggere - senza l'autorizzazione del Titolare/Responsabile del trattamento - stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati personali oggetto del trattamento nonché di consegnare a persone non autorizzate tali documenti.
- L'accesso agli archivi cartacei è limitata al solo personale autorizzato al trattamento dal Titolare/Responsabile del trattamento ai soli dati la cui conoscenza sia strettamente necessaria per adempiere al servizio richiesto.

- In riferimento all'accesso agli archivi - specificatamente individuati dal Titolare/Responsabile del trattamento e/o dal Responsabile – L'azienda utilizza appositi registri di accesso (indicanti tutte le richieste di documentazione, il nominativo dell'incaricato e/o la struttura che inoltra la richiesta, la data e l'ora della richiesta ovvero dell'asportazione dei documenti; i documenti e/o le pratiche di cui si richiede l'asportazione dall'archivio. la data e l'ora della riconsegna dei documenti asportati, il nominativo dell'incaricato e/o la struttura che ha riconsegnato i documenti, se necessario la motivazione di un eventuale ritardo nella consegna).
- Il personale autorizzato deve osservare le procedure adottate dall'azienda in materia di accesso agli archivi selezionato nonché in materia di Privacy e sicurezza delle informazioni.
- LAZIOcrea, ai fini della conservazione/archiviazione dei documenti, mette a disposizione del personale dipendente appositi locali, armadi e cassettiere (archivi) muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro. Le chiavi sono fornite solo ai soggetti autorizzati.

Nel caso di dati sensibili e giudiziari, inoltre, sono state adottate regole più stringenti e maggiori cautele nell'effettuazione dei relativi trattamenti.
Inoltre, ai fini della sicurezza degli archivi cartacei LAZIOcrea ha adottato dispositivi di sicurezza passiva come rilevatori di fumo, allarme, estintori. Inoltre l'incaricato ha l'obbligo di segnalare ogni eventuale disfunzione o anomalia dei menzionati dispositivi.

Regole in ordine alla sicurezza nella cancellazione dei dati

- La cancellazione dei dati personali può essere effettuata solo su autorizzazione del Titolare/Responsabile del trattamento conformemente ai parametri normativi stabiliti dal Regolamento UE (ossia quando la conservazione degli stessi non è più necessaria per legge e/o per gli scopi per cui sono stati raccolti e successivamente trattati, fermo restando l'esercizio del diritto riconosciuto agli interessati alla cancellazione/oblio).
- L'eventuale distruzione/cancellazione dei dati, previa autorizzazione, deve essere effettuata in modo da rendere gli stessi illeggibili. L'azienda ha adottato sistemi meccanici che distruggono i documenti in modo da evitare ogni possibile recupero delle informazioni.
- In caso di cancellazione dei dati memorizzati sui files elettronici, l'azienda ha adottato regolamenti/procedure in ordine alla funzione "svuotamento del cestino in modalità sicura".
- L'azienda ha adottato regole finalizzate a garantire un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento delle attività lavorative nonché finalizzate alla conservazione di determinati atti in archivi ad accesso selezionato e in ordine alle relative modalità di accesso del personale autorizzato.
- Sono, altresì, state adottate regole/procedure in ordine alla sicurezza degli archivi cartacei e gestione protocollo aziendale e istruzioni in ordine alla cancellazione dei dati personali.

5. CODICE COMPORTAMENTALE

Si elencano di seguito le norme comportamentali che il personale dipendente e il management di LAZIOcrea devono rispettare nello svolgimento delle proprie attività lavorative (istruzioni fornite all'interno degli atti di nomina ad "Incaricato del trattamento").

5.1. Regole generali da osservare nello svolgimento delle operazioni di trattamento dei dati personali

Le operazioni di trattamento dei dati personali devono essere effettuate nel rispetto della normativa nazionale ed europea in materia di trattamento dei dati personali ovvero in osservanza dei principi di necessità, liceità, correttezza e proporzionalità ivi contemplati.

Nel dettaglio:

- Il trattamento dei dati deve essere effettuato in modo lecito e corretto.
- I dati personali devono essere raccolti, registrati e trattati unicamente per le finalità inerenti all'attività svolta.
- Le modalità con cui si effettuano i trattamenti devono essere pertinenti e non eccedenti le finalità perseguite (ovvero l'incaricato risulta autorizzato al trattamento dei dati personali al solo fine di effettuare le proprie mansioni lavorative e/o l'incarico affidato).
- Il trattamento dei dati personali deve avvenire solo se necessario allo svolgimento della propria attività lavorativa, escludendo lo stesso quando le finalità perseguite possono essere realizzate mediante l'utilizzo di dati anonimi e/o mediante modalità che permettano di identificare l'interessato solo in caso di necessità.
- I dati personali oggetto di trattamenti devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento compatibilmente con i predetti scopi.
- Risulta necessaria la verifica costante dell'esattezza dei dati, il loro aggiornamento e la loro conservazione nel rispetto delle misure/procedure di sicurezza adottate dall'Azienda.
- L'incaricato è tenuto ad assicurarsi che i dati trattati non vadano dispersi e/o acquisiti, anche in modo incontrollato, da terzi non autorizzati al trattamento.
- Risulta necessaria la verifica costante della completezza e pertinenza dei dati trattati il cui trattamento non deve essere eccedente rispetto alle finalità per le quali sono raccolti o successivamente trattati.
- Devono essere rispettate le misure di sicurezza riportate nei Regolamenti/Procedure Aziendali in materia di trattamento dei dati personali e utilizzo dei mezzi informatici nonché le indicazioni e/o istruzioni fornite dal Titolare del Trattamento e/o dal Responsabile dell'Ufficio Privacy.
- Risulta vietato modificare i trattamenti esistenti e/o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile del Trattamento dei dati personali.

- Le operazioni di trattamenti devono essere effettuate in osservanza delle prescrizioni contenute nel Codice della Privacy nonché nei regolamenti aziendali in materia di Privacy pubblicati sul portale dei dipendenti nell'apposita sezione dedicata alla Privacy).
- L'incaricato del trattamento ha l'obbligo di controllare e custodire i dati personali oggetto del trattamento in modo da evitare o, comunque, ridurre al minimo i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

5.2. Obblighi di riservatezza

L'incaricato del trattamento deve garantire la massima riservatezza in relazione ai dati personali (soprattutto sensibili) di cui venga a conoscenza nell'espletamento delle proprie attività lavorative ed in particolare:

- risulta vietato comunicare e/o diffondere dati personali a terzi non autorizzati al trattamento senza la preventiva autorizzazione del Responsabile del Trattamento dei dati;
- risulta vietato comunicare dati personali ad un collega autorizzato al trattamento in presenza di terzi non autorizzati;
- risulta vietato parlare ad alta voce quando si comunicano dati personali per telefono, evitando comunque che terzi non autorizzati vengano a conoscenza di informazioni personali ascoltando la conversazione;
- l'accesso ai dati dovrà essere limitato all'espletamento delle proprie attività lavorative ed esclusivamente negli orari di lavoro;
- in caso di interruzione, anche temporanea, del lavoro risulta necessario verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le attività, nel cui ambito vengono effettuate le operazioni di trattamento, devono essere svolte secondo le prescrizioni contenute nei Regolamenti/Procedure Aziendali in materia di Privacy e in materia di utilizzo dei mezzi informatici, posta elettronica e internet (pubblicati sul portale dei dipendenti nell'apposita sezione dedicata alla Privacy) nonché secondo le istruzioni e/o raccomandazioni del Responsabile del Trattamento dei dati e/o del Responsabile dell'Ufficio Privacy;
- in caso di incidente di sicurezza che coinvolga dati personali (soprattutto dati sensibili) risulta necessario informare tempestivamente il Responsabile del Trattamento e/o l'Amministratore di Sistema;
- risulta necessario raccogliere, registrare e conservare i dati presenti nei files informatici e nei documenti cartacei avendo cura che l'accesso agli stessi sia reso possibile solo al personale autorizzato;
- qualora giungano richieste telefoniche di dati personali da parte dell'Autorità Giudiziaria o degli Organi di Polizia, risulta necessario assicurarsi circa l'identità del chiamante nonché chiedere l'autorizzazione al Responsabile del Trattamento prima di comunicare i dati stessi;

- risulta opportuno registrare tutte le richieste di comunicazione della documentazione che contiene dati sensibili (eventualmente utilizzare un apposito registro di carico e scarico se autorizzato dal Responsabile del Trattamento);
- risulta necessario distruggere o comunque rendere illeggibili i documenti cartacei non più utilizzati, prima che gli stessi vengano cestinati.

Gli obblighi di cui sopra, relativi alla riservatezza dei dati trattati, ovvero dei dati personali di cui l'incaricato è venuto a conoscenza per ragioni di lavoro, devono essere osservati anche a seguito di modifica dell'incarico e/o di cessazione del rapporto di lavoro.

5.3. Obblighi inerenti al trattamento con l'ausilio di strumenti elettronici

Si elencano di seguito gli obblighi inerenti alle credenziali di autenticazione (password).
L'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata delle proprie credenziali di autenticazione (password) nonché la diligente custodia dei dispositivi elettronici (computer) in uso esclusivo e/o comunque in possesso dell'incaricato.

Nel dettaglio risulta necessario:

– elaborare la password secondo le indicazioni dell'Amministratore di Sistema e/o del Responsabile di Sistemi Informativi e conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (*username*);

– rispettare i profili di autorizzazione attribuiti ai fini dell'accesso ai dati ovvero all'utilizzo di determinati applicativi informatici e/o piattaforme informatiche nell'ambito delle attività lavorative assegnate;

– custodire in modo diligente i dispositivi elettronici in possesso e/o in uso esclusivo.

Al riguardo si precisa quanto segue:

- la parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri, di questi almeno quatto devono essere di natura numerica;
- risulta necessario che la parola chiave non contenga riferimenti agevolmente riconducibili all'incaricato; quindi, la parola chiave non deve essere: il nome o il cognome dell'incaricato, il soprannome, la data di nascita propria, dei figli o degli amici, il nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi, il nome e cognome di personaggi famosi, etc.;
- Risulta inoltre vietato:
  - rivelare la parola chiave a terzi non autorizzati;
  - scrivere la parola chiave in un messaggio di posta elettronica;
  - rivelare la parola chiave al superiore;
  - dare indicazione in merito al formato ed alla lunghezza della parola chiave;
  - svelare la parola chiave su questionari e/o su formulari di sicurezza,

- la parola chiave deve essere modificata dall'incaricato almeno ogni sei mesi (il sistema prevede in automatico la modifica della parola chiave ogni tre mesi); in caso di trattamento di dati sensibili e/o di dati giudiziari la parola chiave deve essere modificata obbligatoriamente ogni tre mesi;

- l'incaricato ha l'obbligo di terminare la sessione di lavoro, al computer, ogni volta che si deve allontanare, anche solo per poco tempo, dal proprio ufficio;

- spetta all'incaricato mettere in atto gli accorgimenti ritenuti più opportune affinché anche in sua assenza, il computer non resti incustodito e/o accessibile a terzi non autorizzati;

- in ogni caso deve essere attivata la funzione *screen saver* qualora l'incaricato si allontani, anche solo per pochi minuti, dal proprio ufficio;

- risulta, inoltre, importante curare la conservazione e la segretezza della parola chiave evitando di trascriverla sul classico *post-it* oppure di tenerla nel portafoglio o trascritta nella prima pagina dell'agenda o della rubrica di ufficio o in qualunque altro posto facilmente intuibile.

(N.B. Al fine di tutelare l'integrità dei dati trattati e memorizzati sui files di rete, si precisa che l'azienda ha adottato un sistema di *back up che* opera in automatico a fine giornata lavorativa.

5.4. Obblighi inerenti ai trattamenti senza l'ausilio di strumenti informatici

Si elencano di seguito le regole principali che l'incaricato deve osservare nelle operazioni di trattamento dei dati personali.

- I documenti che contengono dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione, se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Nel periodo di tempo in cui i documenti che contengono dati personali si trovano al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non deve lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti che contengono dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi ed integri.
- Al termine dell'orario di lavoro, l'incaricato del trattamento deve riportare tutti i documenti che contengono dati personali nei locali (Archivi) individuati per la loro conservazione.
- I documenti (Faldoni, Raccoglitori, Fascicoli, etc.) che contengono dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Risulta necessario adottare ogni cautela affinché persone non autorizzate non vengano a conoscenza dei dati personali contenuti nei documenti utilizzati per lo svolgimento delle mansioni lavorative.

- Per evitare il rischio di divulgazione dei dati personali si deve limitare l'utilizzo di copie fotostatiche. Particolare cautela deve essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato;

Risulta inoltre vietato:

- effettuare copie fotostatiche o di qualsiasi altra natura - non autorizzate dal Responsabile del Trattamento dei dati personali - di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati personali oggetto del trattamento;
- sottrarre, cancellare, distruggere - senza l'autorizzazione del Responsabile del Trattamento dei dati personali - stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati personali oggetto del trattamento;
- consegnare - a persone non autorizzate dal Responsabile del Trattamento dei dati personali - stampe, tabulati, elenchi, rubriche e, più in generale, ogni altro materiale che contiene dati/informazioni personali oggetto del trattamento.

In riferimento, invece, agli obblighi inerenti alla sicurezza degli archivi cartacei nonché alla sicurezza nella cancellazione dei dati si elencano le seguenti regole che l'incaricato deve osservare.

a) Sicurezza Archivi Cartacei

- L'accesso agli archivi cartacei è limitata al solo personale autorizzato al trattamento e ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati.

(N.B. La chiave degli archivi è fornita ai soli soggetti autorizzati).

Nel caso di dati sensibili e giudiziari, inoltre, devono essere osservate le seguenti regole:

- le cartelle o fascicoli o supporti cartacei di vario genere che contengono dati personali devono essere conservati in armadi (Archivi) muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro dall'incaricato del trattamento;
- maggiori cautele devono essere utilizzate per i documenti e/o atti che contengono dati sensibili e giudiziari; in particolare i menzionati dati affidati all'incaricato del trattamento, qualora non vengano utilizzati, devono essere conservati in contenitori chiusi a chiave fino al loro rientro in archivio;

b) Sicurezza nella cancellazione dei dati

- La cancellazione dei dati personali può essere effettuata – previa autorizzazione del Responsabile del Trattamento - quando la conservazione degli stessi non è più necessaria per legge e/o per gli scopi per cui sono stati raccolti e successivamente trattati.
- I dati personali possono essere cancellati anche su richiesta dell'interessato, sempre che la conservazione non sia necessaria per legge e/o per la gestione del rapporto di lavoro (e/o contrattuale nel caso di consulenti e/o fornitori), sempre previa autorizzazione del Responsabile del Trattamento.
- L'eventuale distruzione dei dati deve essere effettuata con sistemi meccanici o automatizzati in modo da evitare ogni possibile recupero. In caso di cancellazione dei dati

memorizzati sui files elettronici, l'incaricato è tenuto al rispetto dei regolamenti aziendali in ordine alla funzione "svuotamento del cestino in modalità sicura".

- I documenti che contengono dati personali forniti all'Azienda per l'esecuzione della propria attività lavorativa dovranno essere restituiti e/o cancellati – previa autorizzazione del Responsabile del Trattamento - alla cessazione del rapporto di lavoro e/o comunque in tutti i casi in cui il trattamento dei dati personali non risulta essere necessario ai fini dell'espletamento delle mansioni lavorative assegnate, salvo diversa prescrizione di legge.

Per quanto non previsto nel presente documento, si precisa che sarà cura del Responsabile/Titolare del Trattamento fornire ogni altra istruzione e/o raccomandazione in ordine alle operazioni di trattamento dei dati personali, alla gestione e custodia degli stessi nel rispetto della vigente normativa in materia di Privacy nonché nel rispetto delle normative applicabili alle diverse tipologie di attività effettuate nei singoli uffici/Aree (es. normativa in materia di Archivio, in materia di Salute e Sicurezza sui luoghi di lavoro, in materia di atti e documenti amministrativi, etc.).

***

Per ogni altra misura di sicurezza e/o istruzione e/o raccomandazione non contemplate nel presente documento, si rinvia ai Regolamenti/Procedure Aziendali in materia di trattamento dei dati personali pubblicati sui siti Internet e intranet nelle apposite sezioni (MOG, Sistemi di qualità, etc.).

5.5 Istruzioni specifiche in ordine alle operazioni di trattamento dei dati personali per conto della Regione Lazio ed Enti alla stessa collegati.

Le operazione di trattamento dei dati personali devono essere effettuate nel rispetto della vigente normativa nazionale ed europea in materi di trattamento dei dati personali (di cui al D.Lgs. n. 196/2003, s.m.i. e al Regolamento dell'Unione Europea n. 679/2016) ovvero in osservanza delle prescrizioni e dei principi ivi contemplati (Principi di necessità, liceità, trasparenza, correttezza e proporzionalità).

Le istruzioni di seguito riportate sono vincolanti per il personale dipendente se correlate al servizio svolto a supporto dell'amministrazione regionale (specificato nel POA).

Nel dettaglio.

- Il trattamento dei dati deve essere effettuato in modo lecito e corretto.

- I dati personali devono essere trattati unicamente ed esclusivamente per le finalità inerenti al servizio svolto a supporto della Regione Lazio (servizio riferito al POA)

- I dati personali, quindi, devono essere raccolti, registrati e successivamente trattati unicamente per le finalità inerenti al servizio svolto (attività connesse alla funzione amministrativa).

- Le modalità con cui si effettuano i trattamenti devono essere pertinenti e non eccedenti le finalità perseguite (ovvero l'incaricato è autorizzato al trattamento dei dati personali al solo fine di effettuare le attività lavorative assegnate).

- Il trattamento dei dati personali deve avvenire solo se necessario allo svolgimento della propria attività lavorativa, escludendo lo stesso quando le finalità perseguite possono essere realizzate mediante l'utilizzo di dati anonimi e/o mediante modalità che permettano di identificare l'interessato solo in caso di necessità (principio di limitazione del trattamento dei dati) secondo le istruzioni impartite dal Responsabile della struttura regionale di riferimento.

- I dati personali oggetto di trattamenti devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento compatibilmente con i predetti scopi.

- Il trattamento dei dati deve essere effettuato secondo il principio di trasparenza, ovvero deve essere assicurata la consapevolezza dell'interessato in ordine al trattamento dei dati che lo riguardano.

- Se necessario e correlato alle mansioni lavorative svolte, l'incaricato deve verificare costantemente – secondo le istruzioni fornite dal Responsabile della struttura regionale di riferimento– l'esattezza dei dati, il loro aggiornamento e la loro conservazione nel rispetto delle misure/procedure di sicurezza adottate dalla Regione Lazio in materia di Privacy, di utilizzo degli strumenti informatici e sicurezza delle informazioni.

- L'incaricato è tenuto ad assicurarsi che i dati trattati non vadano dispersi e/o acquisiti, anche in modo incontrollato, da terzi non autorizzati al trattamento.

- Se necessario e correlato alle mansioni svolte, l'incaricato deve verificare costantemente – secondo le istruzioni fornite dal Responsabile della struttura regionale di riferimento - la completezza e pertinenza dei dati trattati il cui trattamento non deve essere eccedente rispetto alle finalità per le quali sono raccolti e/o successivamente trattati.

- E' vietato modificare i trattamenti esistenti e/o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Responsabile della struttura regionale di riferimento.

- In caso di incidente di sicurezza che coinvolga dati personali (soprattutto dati sensibili) l'incaricato ha l'obbligo prescritto dalla legge di informare tempestivamente il Responsabile della struttura regionale di riferimento. In particolare, si elencano a titolo esemplificativo e non esaustivo i casi di violazione dei dati personali e/o incidente di sicurezza: distruzione - accidentale e/o illecita - perdita, modifica, divulgazione e accessi non autorizzati ai dati trasmessi, conservati o comunque trattati.

- Devono essere rispettate le indicazioni e/o le istruzioni fornite dal Responsabile della Protezione dei dati della Regione Lazio e/o dal Responsabile della struttura regionale di riferimento. Le operazioni di trattamento devono essere effettuate in osservanza della normativa nazionale ed europea in materia di Privacy nonché nel rispetto delle

procedure/regolamenti adottati dalla amministrazione regionale in materia di trattamento dei dati personali, utilizzo degli strumenti informatici/elettronici e sicurezza delle informazioni.

- Nel caso in cui devono essere effettuate operazioni di trattamento consistenti in comunicazioni/divulgazioni di dati all'esterno, l'incaricato ha l'obbligo di osservare le istruzioni impartite dal Responsabile della struttura regionale di riferimento, previa autorizzazione.

- Al fine di ottemperare agli obblighi relativi all'informativa e al consenso, l'incaricato ha l'obbligo di osservare le istruzioni impartite dal Responsabile della struttura regionale di riferimento, previa autorizzazione.

- In caso di trattamenti che esulano dall'ordinaria gestione ed esecuzione delle attività lavorative affidate (soprattutto comunicazione di dati all'interno degli uffici), l'incaricato ha l'obbligo di informare il Responsabile della struttura regionale di riferimento al fine di garantire la corretta osservanza delle prescrizioni di cui alla normativa in materia di Privacy.

- Se correlato alle mansioni lavorative affidate, l'incaricato deve supportare il Responsabile della struttura regionale di riferimento nel garantire agli interessati del trattamento l'esercizio dei diritti contemplati dal Regolamento U.E. 679/2016 nel rispetto delle procedure aziendali adottate (Diritto all'oblio, alla limitazione del trattamento, alla rettifica, all'aggiornamento, alla portabilità dei dati, di opposizione, di non subire profilazione, etc.). Al riguardo si precisa che sarà cura del Responsabile della struttura regionale di riferimento e/o del DPO della Regione Lazio fornire ulteriori istruzioni in merito.

- Se richiesto e correlato alle attività lavorative assegnate, l'incaricato deve supportare il Responsabile della struttura regionale di riferimento nella predisposizione ed implementazione delle misure di sicurezza, tecniche ed organizzative, ai fini della corretta osservanza ed attuazione della normativa in materia di Privacy

- Se necessario e correlato all'attività lavorativa svolta, l'incaricato deve procedere all'eventuale cancellazione, limitazione del trattamento, pseudonimizzazione e/o cifratura dei dati nel rispetto delle istruzioni impartite dal Responsabile della struttura regionale di riferimento e/o dal DPO della Regione Lazio in linea con le procedure/regolamenti adottati nonché nel rispetto delle misure di sicurezza prescritte dalla normativa in materia di Privacy.

(Nota: per ulteriori approfondimenti si rinvia ai regolamenti/procedure/policy adottate dalla Regione Lazio)

5.6. Obblighi di riservatezza in ordine ai dati trattati per conto della Regione Lazio ed Enti alla stessa collegati.

L'incaricato del trattamento deve garantire la massima riservatezza in relazione ai dati personali trattati e/o di cui venga a conoscenza nell'espletamento delle proprie attività lavorative. L'obbligo

di riservatezza deve essere rispettato anche in relazione alle credenziali di autenticazione assegnate (password),

Nel dettaglio l'incaricato deve:

- chiedere l'autorizzazione al Responsabile della struttura regionale di riferimento - qualora giungano richieste anche da parte di uffici interni – per effettuare comunicazioni e/o accessi ai dati personali e/o alla documentazione che contiene i dati stessi;
- in caso di interruzione, anche temporanea, delle attività lavorative, adottare tutti gli accorgimenti ritenuti più opportuni al fine di evitare che i dati trattati non siano accessibili a terzi non autorizzati;
- raccogliere, registrare e conservare i dati presenti nei files informatici e/o nei documenti cartacei avendo cura che l'accesso agli stessi sia reso possibile solo al personale autorizzato;
- qualora giungano richieste di comunicazione di dati personali da parte dell'Autorità Giudiziaria e/o degli Organi di Polizia, avvertire comunque il Responsabile della struttura regionale di riferimento e/o DPO della Regione Lazio di lavoro prima di comunicare i dati stessi;
- fermo restando i divieti di cancellazione e/o obblighi di conservazione stabiliti dalle normative di legge, distruggere o comunque rendere illeggibili i documenti cartacei - che contengono dati personali - non più utilizzati, prima che gli stessi vengano cestinati.

Inoltre è vietato:

- comunicare e/o diffondere dati personali a terzi non autorizzati al trattamento senza l'autorizzazione del Responsabile della struttura regionale di riferimento e, ove necessario, previo rilascio dell'informativa obbligatoria e/o prestazione del consenso da parte degli interessati al trattamento;
- comunicare dati personali ad un collega autorizzato al trattamento in presenza di terzi non autorizzati;
- parlare ad alta voce quando si comunicano i dati personali (anche per telefono), evitando comunque che terzi non autorizzati vengano a conoscenza di informazioni personali ascoltando la conversazione;
- comunicare ad un collega autorizzato al trattamento e/o ad un terzo non autorizzato le proprie credenziali di autenticazione.

Gli obblighi relativi alla riservatezza dei dati trattati dovranno essere osservati anche a seguito di cambiamento delle mansioni lavorative assegnate (es. mobilità), cessazione del rapporto di lavoro e/o temporanea sospensione delle attività lavorative (es. aspettativa, maternità e/o congedi parentali).

***

Il trattamento dei dati deve avvenire assicurando la tutela della riservatezza, integrità e disponibilità dei dati stessi, nonché nel rispetto della dignità della persona dell'interessato al trattamento. In particolare le operazioni di trattamento devono essere effettuate eliminando ogni occasione di impropria e/o illegittima conoscibilità di informazioni personali da parte di terzi non autorizzati al trattamento.

Qualora il trattamento dei dati sia effettuato in violazione dei principi sopra menzionati, di quanto disposto dalla normativa in materia di Privacy, e delle istruzioni impartite dal Responsabile della struttura regionale di riferimento, l'incaricato ha l'obbligo stabilito dalla normativa stessa di informare tempestivamente il Responsabile stesso e/o il DPO della Regione Lazio al fine di procedere eventualmente al blocco dei dati trattati (vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del trattamento medesimo) e/o consentire l'osservanza degli obblighi di legge relativi alle notifiche al Garante Privacy e/o agli interessati (c.d. data breach).

5.7. Obblighi inerenti al trattamento dei dati per conto della Regione Lazio ed Enti alla stessa collegati con l'ausilio di strumenti elettronici/automatizzati.

Le istruzioni di seguito riportate sono vincolanti per il personale dipendente ove correlate all'attività lavorativa assegnata.

In base a quanto stabilito dalla normativa nazionale ed europea in materia di Privacy per le operazioni di trattamento dei dati personali effettuate con strumenti elettronici/automatizzati, l'incaricato del trattamento deve osservare le misure di sicurezza adottate dall'amministrazione regionale di riferimento e specificate nei relativi regolamenti e/o procedure in materia di privacy, di utilizzo di strumenti informatici, internet e posta elettronica nonchè in materia di sicurezza delle informazioni (ISO 27001).

Nel dettaglio si riportano di seguito gli obblighi inerenti all'utilizzo delle credenziali di autenticazione (UserID e Password) assegnate dai Responsabili delkle strutture regionali di riferimento.

L'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata delle credenziali di autenticazione (password) assegnate nonché la diligente custodia dei dispositivi elettronici (computer) in uso esclusivo e/o comunque in possesso dell'incaricato.

Nel dettaglio risulta necessario:

- Elaborare la password secondo le indicazioni fornite dal Responsabile della struttura amministrativa di riferimento e/o riportate nei regolamenti/procedure adottate dalla Regione Lazio e conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (username).
- Rispettare i profili di autorizzazione attribuiti dal Responsabile della struttura regionale di riferimento ai fini dell'accesso ai dati e ai sistemi (ovvero all'utilizzo di determinati applicativi informatici e/o piattaforme informatiche e/o data-base nell'ambito del servizio svolto e specificato nel POA).

– Custodire in modo diligente i dispositivi elettronici in possesso e/o in uso esclusivo.

Inoltre, si precisa quanto segue:

- La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri, di cui almeno quatto devono essere di natura numerica.
- Risulta necessario che la parola chiave non contenga riferimenti agevolmente riconducibili all'incaricato; quindi, la parola chiave non deve essere: il nome o il cognome dell'incaricato, il soprannome, la data di nascita propria, dei figli o degli amici, il nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi, il nome e cognome di personaggi famosi, etc.

E' vietato:

- rivelare la parola chiave a terzi non autorizzati;
- scrivere la parola chiave in un messaggio di posta elettronica;
- rivelare la parola chiave al superiore;
- dare indicazione in merito al formato ed alla lunghezza della parola chiave;
- svelare la parola chiave su questionari e/o su formulari di sicurezza.

La parola chiave deve essere modificata dall'incaricato almeno ogni sei mesi, in caso di trattamento di dati sensibili e/o di dati giudiziari la parola chiave deve essere modificata obbligatoriamente ogni tre mesi.

Si riportano di seguito ulteriori istruzioni in ordine all'utilizzo di strumenti elettronici.

- ✓ L'incaricato ha l'obbligo di terminare la sessione di lavoro, al computer, ogni volta che si deve allontanare, anche solo per poco tempo, dal proprio ufficio.
- ✓ Spetta all'incaricato mettere in atto gli accorgimenti ritenuti più opportuni affinché anche in sua assenza, il computer non resti incustodito e/o accessibile a terzi non autorizzati.
- ✓ In ogni caso deve essere attivata la funzione screen saver qualora l'incaricato si allontani, anche solo per pochi minuti, dal proprio ufficio.
- ✓ Risulta, inoltre, importante curare la conservazione e la segretezza della parola chiave evitando di trascriverla su supporto cartaceo precario o visibile (es. post-it) oppure di tenerla nel portafoglio o trascritta nella prima pagina dell'agenda o della rubrica di ufficio o in qualunque altro posto facilmente intuibile;

Al fine di tutelare l'integrità e il ripristino della disponibilità dei dati trattati e memorizzati sui files di rete, l'incaricato è obbligato al rispetto del sistema di *back up* regionale.

5.8. Obblighi inerenti ai trattamenti dei dati per conto della Regione Lazio ed Enti alla stessa collegati senza l'ausilio di strumenti informatici/automatizzati

Le istruzioni di seguito riportate sono vincolanti per il personale dipendente se correlate all'attività lavorativa assegnata.

Per le operazioni di trattamento dei dati personali effettuate senza l'ausilio di strumenti elettronici, l'incaricato del trattamento deve osservare le misure di sicurezza adottate dalla Regione Lazio nonché le istruzioni impartite dal Responsabile della struttura regionale di riferimento. In particolare l'incaricato ha l'obbligo di rispettare le procedure e/o i regolamenti in materia di Privacy, sicurezza delle informazioni e in materia di conservazione di atti e documenti amministrativi, di archivio e di protocollo.

Nel dettaglio si elencano di seguito le regole principali che l'incaricato deve osservare nelle operazioni di trattamento dei dati personali.

- I documenti che contengono dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione, se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Nel periodo di tempo in cui i documenti che contengono dati personali si trovano al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non deve lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti che contengono dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi ed integri.
- Al termine dell'orario di lavoro, l'incaricato del trattamento deve riportare tutti i documenti che contengono dati personali nei locali (Archivi) individuati per la loro conservazione.
- I documenti (Faldoni, Raccoglitori, Fascicoli, etc.) che contengono dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Risulta necessario adottare ogni cautela affinché persone non autorizzate non vengano a conoscenza dei dati personali contenuti nei documenti utilizzati per lo svolgimento delle attività lavorative.
- Per evitare il rischio di divulgazione dei dati personali si deve limitare l'utilizzo di copie fotostatiche. Particolare cautela deve essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato.

Risulta inoltre vietato:

- Effettuare copie fotostatiche o di qualsiasi altra natura - non autorizzate dal Responsabile della struttura regionale di riferimento - di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Sottrarre, cancellare, distruggere - senza l'autorizzazione del Responsabile della struttura regionale di riferimento - stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Consegnare - a persone non autorizzate dal Responsabile della struttura regionale di riferimento - stampe, tabulati, elenchi, rubriche e, più in generale, ogni altro materiale che contiene dati/informazioni personali oggetto del trattamento.

In riferimento, invece, agli obblighi inerenti alla sicurezza degli archivi cartacei nonché alla sicurezza nella cancellazione dei dati si elencano le seguenti regole che l'incaricato deve osservare secondo le istruzioni impartite dal Responsabile della struttura regionale di riferimento e/o previa autorizzazione dello stesso.

Sicurezza Archivi Cartacei

- L'accesso agli Archivi cartacei è limitata al solo personale autorizzato al trattamento e ai soli dati la cui conoscenza sia strettamente necessaria per adempiere alle attività lavorative assegnate.

La chiave degli archivi è fornita ai soli soggetti autorizzati.

Nel caso di dati sensibili e giudiziari, inoltre, devono essere osservate le seguenti regole:

- Le cartelle o fascicoli o supporti cartacei di vario genere che contengono dati personali devono essere conservati in armadi (Archivi) muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro dall'incaricato del trattamento.
- Maggiori cautele devono essere utilizzate per i documenti e/o atti che contengono dati sensibili e giudiziari; in particolare i menzionati dati affidati all'incaricato del trattamento, qualora non vengano utilizzati, devono essere conservati in contenitori chiusi a chiave (es. cassettiere) fino al loro rientro in archivio.

Ai fini della sicurezza degli Archivi cartacei, la Regione Lazio ha adottato dispositivi di sicurezza passiva come rilevatori di fumo, allarme, estintori.

Sicurezza nella cancellazione dei dati

- La cancellazione dei dati personali può essere effettuata – previa autorizzazione del Responsabile della struttura regionale di riferimento - quando la conservazione degli stessi non è più necessaria per legge e/o per gli scopi per cui sono stati raccolti e successivamente trattati (rispettare i tempi di conservazione previsti dalla legge per atti e documenti amministrativi).
- I dati personali possono essere cancellati anche su richiesta dell'interessato al trattamento (anche ai fini dell'esercizio del diritto all'oblio) - sempre che la conservazione non sia necessaria per legge e/o per la gestione del rapporto di lavoro (e/o contrattuale nel caso di consulenti e/o fornitori) - e comunque previa autorizzazione del Responsabile della struttura regionale di riferimento.
- L'eventuale distruzione dei dati deve essere effettuata con sistemi meccanici o automatizzati in modo da evitare ogni possibile recupero. In caso di cancellazione dei dati memorizzati sui files elettronici, l'incaricato è tenuto al rispetto dei regolamenti/procedure aziendali (es. utilizzo funzione "svuotamento del cestino in modalità sicura") nonché delle istruzioni impartite dal Responsabile della struttura regionale di riferimento.
- I documenti che contengono dati personali forniti per l'erogazione di servizi a supporto dell'amministrazione regionale dovranno essere restituiti e/o cancellati – previa autorizzazione del Responsabile della struttura regionale di riferimento – alla cessazione/interruzione del servizio richiesto e/o comunque in tutti i casi in cui il

trattamento dei dati personali non risulta essere più necessario per il perseguimento delle finalità suindicate, salvo diversa prescrizione di legge.

In ogni caso l'incaricato del trattamento ha l'obbligo di controllare e custodire i dati personali oggetto del trattamento in modo da evitare o, comunque, ridurre al minimo i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato dal Responsabile della struttura regionale di rifermento. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate su istruzione del Responsabile stesso. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate dal Responsabile della struttura regionale di riferimento.

Per quanto non previsto sopra, si precisa che sarà cura del Titolare del trattamento (Regione Lazio), anche per mezzo del Responsabile della struttura amministrativa regionale di riferimento, fornire ogni altra istruzione e/o raccomandazione in ordine alle operazioni di trattamento dei dati personali, alla gestione e custodia degli stessi nel rispetto della vigente normativa in materia di Privacy nonché nel rispetto delle normative applicabili alle attività delle strutture amministrative regionali (es. normativa in materia di Archivio, in materia di Sicurezza delle informazioni, in materia di Salute e Sicurezza sui luoghi di lavoro, in materia di conservazione di atti e documenti amministrativi, etc.).

Le suindicate istruzioni sono vincolanti anche in caso di cessazione del rapporto di lavoro (anche interruzione temporanea delle attività lavorative come ad es. nei casi di aspettativa, congedi parentali, maternità, etc.) e/o cambiamento delle mansioni affidate. E' vietato comunicare e/o divulgare dati personali di cui l'incaricato è venuto a conoscenza nell'espletamento delle mansioni lavorative assegnate.

6 DOCUMENTI PUBBLICATI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Si riportano di seguito i documenti pubblicati sul sito internet aziendale (la maggior parte dei quali risultano essere anche pubblicati sul portale dei dipendenti/sito intranet) in osservanza dalla normativa in materia di Privacy.

6.1 Documenti predisposti e pubblicati in osservanza degli obblighi informativi prescritti dall'art. 13 e 14 Regolamento UE 679/2016 (GDPR)

Si elencano di seguito i documenti pubblicati sul sito internet aziendale (la maggior parte dei quali risultano essere anche pubblicati sul portale dei dipendenti/sito intranet) in osservanza dalla normativa in materia di Privacy, con particolare riferimento agli obblighi inerenti alle pubblicazioni e all'informativa prescritti dai suindicati articoli del GDPR.

(Nota: al riguardo, come specificato di seguito, si evidenzia che le informative sotto elencate erano state precedentemente predisposte e pubblicate in osservanza della normativa nazionale in materia di Privacy di cui al D.Lgs 196/2003 (c.d. Codice

della Privacy). Successivamente sono state aggiornate e rivisitate in osservanza dei vigenti parametri normativi di cui al Regolamento UE).

- ✓ Sezione Privacy. Informativa ai sensi degli articoli 13 e 14 Regolamento UE 679/2016 (per i dipendenti, i collaboratori equiparati ai dipendenti e i consulenti di LAZIOcrea SpA (pubblicato anche sul sito intranet – portale dipendenti) in linea con gli obblighi previsti dalla normativa in materia di *Anticorruzione e Trasparenza*.
- ✓ Sezione Privacy. Informativa ai sensi degli articoli 13 e 14 Regolamento UE 679/2016 sul trattamento dei dati personali relativi ai fornitori di LAZIOcrea SpA. in linea con gli obblighi previsti dalla normativa in materia di *Anticorruzione e Trasparenza*.

[Nota. Al riguardo si precisa che determinate informazioni personali riguardanti i Consulenti esterni, i collaboratori equiparati ai dipendenti, i Dirigenti, etc. sono state (e/o potrebbero essere) pubblicate sul sito internet aziendale in osservanza degli obblighi previsti dalla normativa c.d. "Anticorruzione e Trasparenza" di cui al D.Lgs. n. 33/2013 (Testo Unico sulla Trasparenza) e alla Legge n. 190/2012 (normativa anticorruzione). Quindi, si è provveduto a predisporre un'informativa nella quale si comunica che l'Azienda procede alla pubblicazione delle sole informazioni personali prescritte dalla legge in osservanza dei principi di necessità, di trasparenza, di legalità e, infine, di rispondenza e non eccedenza contemplati dalla vigente normativa sulla Privacy].

- ✓ Sezione denominata "*Società Trasparente*". Informativa sulla Privacy relativa al riutilizzo dei dati personali pubblicati in ottemperanza alla normativa sulla Trasparenza nelle Pubbliche Amministrazioni.

(Nota: In proposito si evidenzia che in relazione agli obblighi di pubblicazione di atti e informazioni sul web previsti dal D.Lgs. 14 Marzo 2013, n. 33 recante "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni", si è provveduto a predisporre - in ottemperanza alla normativa di cui al D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" nonché ai principi e alle cautele definite nelle "Linee Guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" adottate dal Garante per la protezione dei dati il 15 Maggio 2014 ai sensi dell'art. 154, comma 1, lettera h) del D.Lgs. n. 196/2003 – un'informativa circa il riutilizzo dei dati personali pubblicati in linea con le condizioni previste dalla normativa vigente sul riuso dei dati pubblici (direttiva comunitaria 2003/98/CE e D.Lgs n. 36/2006 di recepimento della stessa) sempre nel rispetto delle norme in materia di protezione dei dati personali)

- ✓ Sezione denominata "*Società Trasparente*". Informativa relativa all'utilizzo dei Cookies in linea con il Provvedimento del Garante della Privacy del 8 Maggio 2014;
- ✓ Sezione Privacy. Modulo per l'esercizio dei diritti dell'interessato al trattamento dei dati contemplati dal Regolamento UE 679/2016
- ✓ Sezione denominata "*Società Trasparente*". Informativa relativa alla raccolta e al successivo trattamento dei dati afferenti ai docenti/tutor - iscritti al relativo albo - ai fini delle attività formative del personale dipendente aziendale e regionale nonché ai fini dell'esecuzione dei progetti.
- ✓ Sezione Privacy. Informativa sulla Videosorveglianza ai sensi dell'Art. 14 Regolamento UE 679/2016 relativa al trattamento dei dati personali (immagini raccolte e registrate) effettuato per mezzo delle telecamere istallate presso la sede di via del Serafico.

6.2 Regolamenti e/o procedure adottate dalla LAZIOcrea in osservanza della normativa in materia di Privacy, ivi compresi i Provvedimenti Generali e le linee guida adottati dal Garante della Protezione dei dati in riferimento a specifici settori.

Si elencano di seguito i regolamenti/procedure adottati da LAZIOcrea - pubblicati sul sito internet, alcuni anche pubblicati sul portale dei dipendenti/sito intranet, nelle apposite sezioni dedicate alla Privacy - in osservanza dalla normativa in materia di protezione dei dati personali e utilizzo di strumenti informatici.

- ✓ Sezione denominata "*Società Trasparente*" e "*Sezione Privacy*". Sistema Privacy in ordine al trattamento dei dati personali" adottato dall'azienda in osservanza del D.Lgs 196/2003 e s.m.i. (pubblicato all'interno dell'Allegato 3 del Modello Organizzativo di Gestione e Controllo - TU Regolamenti e Procedure) . Sostituito dal presente documento predisposto in linea con i parametri di cui al Regolamento UE

(Nota: il suindicato sistema riporta le regole comportamentali vincolanti per il personale dipendente e il management nelle operazioni di trattamento dei dati personali).

- ✓ Sezione denominata "*Società Trasparente*". "*Regolamento Aziendale in ordine all'utilizzo degli strumenti informatici, posta elettronica, internet e dei servizi di telefonia"*, adottato dall'azienda in osservanza della normativa in materia di Privacy - con particolare riferimento all'Allegato B del D.Lgs 196/2003 e conformemente alle linee guida del Garante della Protezione dei dati in materia di navigazione internet e utilizzo della posta elettronica del 1 Marzo 2007 - anche pubblicato all'interno dell'Allegato 3 del Modello Organizzativo di Gestione e Controllo - TU Regolamenti e Procedure.
- ✓ Sezione Privacy. "Regolamento Aziendale sulla Videosorveglianza*"* adottato da LAZIOcrea in osservanza del Provvedimento Generale del Garante della protezione dei dati dell'8 Aprile 2010.

(Nota: nella sezione denominata "Società Trasparente" (organizzazione uffici) era stata pubblicata la declaratoria delle attività svolte dall'Area Sicurezza sul lavoro e Privacy (Microstruttura pubblicata il 27 Giugno 2016 e successivamente aggiornata).

- ✓ Sezione Procedure – Sistema di Gestione per la qualità ISO 9001:2015. Sono pubblicate le procedure gestionali certificate inerenti alle gestione delle tecnologie infrastrutturali.

6.3 Pubblicazione dei riferimenti normativi in materia di protezione dei dati personali (Normativa Nazionale e Normativa Europea)

- ✓ Codice in materia di protezione dei dati personali c.d. "*Codice della Privacy*" (ovvero il testo normativo del D.Lgs. 196/2003, pubblicato anche sul sito intranet-portale dipendenti).
- ✓ "*Disciplinare tecnico in materia di misure minime di sicurezza*" 'allegato B) del D.Lgs. 196/2003 (pubblicato anche sul sito intranet-portale dipendenti).

- ✓ "*Pacchetto Protezione dei dati*"; in particolare il predetto documento riporta il testo normativo del Regolamento in materia di Privacy dell'Unione Europea 2016/679 entrato in vigore il 25 Maggio 2016 e il cui termine ultimo di attuazione è stato fissato il 25 Maggio 2018 (testo ripreso dal sito istituzionale del Garante della protezione dei dati)

7 ALLEGATI

Si allegano di seguito i moduli utilizzati per la designazione degli incaricati del trattamento ai sensi della normativa nazionale ed europea in materia di protezione dei dati personali di cui agli articoli 30 D.Lgs 196/2003 e 29 Regolamento UE 679/2016.
In particolare si è ritenuto opportuno predisporre due moduli differenziati in base alla tipologia di attività lavorativa effettuata dal personale di LAZIOcrea incaricato del trattamento.

(Nota: il primo modulo è utilizzato per la nomina del personale incaricato di attività aziendali interne e/o servizi a supporto della Regione Lazio gestiti autonomamente da LAZIOcrea. Il secondo modulo è utilizzato per la nomina del personale incaricato dei servizi a supporto della Regione Lazio presso le sedi amministrative della stessa e sotto il diretto controllo dei Dirigenti Responsabili delle diverse strutture dell'amministrazione regionale)

All. n. 1. Atto di Nomina ad "*incarico del trattamento dei dati personali*" in attuazione della normativa nazionale ed europea in materia di Privacy.

La LAZIOcrea SpA con sede in 00142 Roma, via del Serafico n.107 -- Titolare del trattamento dei dati personali afferenti al proprio personale dipendente, ai consulenti e ai fornitori esterni (ivi compresi i docenti/tutor esterni che effettuano attività formative nell'interesse della società stessa) ai sensi della normativa nazionale e europea in materia di Privacy di cui all'28 D.Lgs.196/2003 e all'art. 4, par. 7) Regolamento UE n. 679/2016 nonché in qualità di Responsabile del Trattamento dei dati personali della Regione Lazio ed Enti collegati ai sensi degli articoli 29 D.Lgs 196/203 e 4, par) 8) e 28 del Regolamento UE. – rappresentata per il presente atto dal Presidente legale rappresentante pro tempore Dott. Umena Andrea domiciliato per la carica presso la suddetta sede aziendale.

VISTO

Il decreto legislativo 30 giugno 2003, n. 196 c.d. "Codice in materia di protezione dei dati personali",

Il Regolamento dell'Unione Europea n. 679/2016.
Ed in particolare:
-Il combinato disposto degli articoli 4 comma 1 lett f) e 28 del D.Lgs 196/2003 e degli articoli 4 e 26 Regolamento UE 679/2016 che definiscono il Titolare del trattamento come la persona fisica, la persona giuridica, la pubblica amministrazione, o qualsiasi altro ente, associazione od organismo anche periferico cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

-Il combinato disposto degli articoli 29, comma 5 D.Lgs 196/2003 e 28 Regolamento UE 679/2016 che prevedono "Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni";

-L'art. 4, comma 1, lett. H) D.Lgs 196/2003 che definisce la figura degli incaricati come "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".

-L'art. 30 D.Lgs 196/2003 che prescrive al comma 1. "le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile attenendosi alle istruzioni impartite"; al comma 2 "la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima".

- Il combinato disposto articoli 4 parag. 10 e art. 29 Regolamento UE 679/2016 che individuano la figura degli autorizzati al trattamento sotto l'autorità diretta del Titolare e/o del Responsabile del trattamento, ossia coloro che devono essere istruiti in tal senso (figura riconducibile a quella dell'incaricato del trattamento prevista specificatamente dalla normativa nazionale sulla Privacy di cui al suindicato art. 30)

CONSIDERATO

-Che il personale assegnato all'Area _____facente capo alla Direzione _____ (vedi organigramma e microstruttura aziendale pubblicati), nello svolgimento delle attività lavorative assegnate, tratta i dati personali (indicare la categoria di dati tra: comuni, sensibili e giudiziali afferenti a _____(indicare i soggetti a cui si riferiscono i dati es dati rientranti nella sfera di titolarità _____(della LAZIOcrea come ad es il personale dipendente e/o i dati rientranti nella sfera di titolarità della Regione LAZIO e degli Enti alla stessa collegati es. assistiti/pazienti delle strutture sanitarie e/o della Regione Lazio e/o Enti alla stessa collegati).

- Che sono trattati le seguenti categorie di dati _____(indicare se comuni, sensibili e giudiziari). In particolare, a titolo esemplificativo e non esaustivo, si riportano le tipologie di dati trattati_____(indicare la tipologia es dati anagrafici e/o residenziali e/o afferenti alle malattie degli assistiti del sistema sanitario e/o utenti della Regione Lazio, e/o del Personale dipendente e/o fornitori di LAZIOcrea, etc).

- Che la predetta attività lavorativa, comportando un trattamento costante di dati/informazioni personali, rientra nell'ambito di applicazione della normativa in materia di Privacy. In particolare il personale che tratta i dati personali nell'esecuzione delle proprie attività lavorative deve essere designato, per iscritto, incaricato del trattamento e/o autorizzato e istruito secondo i vigenti parametri di cui alla normativa europea.

- Che, in osservanza del Regolamento Europeo sulla Privacy, il Titolare e/o il Responsabile del trattamento deve garantire la riservatezza dei dati trattati, quindi gli addetti al trattamento sono obbligati al rispetto dei relativi obblighi (riportati di seguito).

RITENUTO

Pertanto di dover procedere alla nomina del personale assegnato – in base alla vigente microstruttura – all'Area _____facente capo alla Direzione _____ ad "*incaricato del trattamento dei dati personali*" ai sensi di legge.

Inoltre la necessità di impartire le istruzioni (riportate di seguito) al personale addetto al trattamento in ordine alla corretta osservanza della normativa nazionale e europea in materia di privacy

NOMINA

Elenco nominativo

.....

.....

INCARICATI DEL TRATTAMENTO

dei dati personali – rientranti nella sfera di titolarità della LAZIOcrea ai sensi degli articoli 28 del D.Lgs 196/2003 e 26 del Regolamento U.E. 679/2016 e/o della Regione Lazio – nell'ambito dell'esecuzione delle attività lavorative di competenza dell'Area Privacy.(vedi organigramma e microstruttura aziendale pubblicati).

La presente nomina è da intendersi valida solo per le tipologie di trattamento – tra quelle contemplate dall'art. 4 lett. A) del D.Lgs 196/2003 e dall'art. 4 paragrafo 2) del Regolamento U.E. 679/2016 – necessarie ai fini dello svolgimento delle attività lavorative assegnate e secondo le modalità e istruzioni riportate nel presente atto e/o impartite dal Responsabile dell'Area.

In particolare gli incaricati designati con il presente atto possono effettuare solo quelle categorie di trattamento – ovvero operazioni o complesso di operazioni svolte sui dati con o senza l'ausilio di strumenti elettronici/automatizzati – espressamente autorizzate dal Responsabile dell'Area _____ (e possono accedere ai sistemi informatici/applicativi, data base, cartelle condivise, Archivi per conservazione dei documenti cartacei) solo previa assegnazione di apposite credenziali di autenticazione in linea con il profilo di autorizzazione attribuito.

A tal fine si forniscono di seguito istruzioni e raccomandazioni in ordine alla corretta effettuazione delle operazioni di trattamento dei suindicati dati personali in osservanza della normativa in materia di Privacy.

Istruzioni in ordine alle operazioni di trattamento dei dati personali
Le istruzioni di seguito riportate sono vincolanti per il personale dipendente se correlate all'attività lavorativa assegnata.

Le operazione di trattamento dei dati personali devono essere effettuate nel rispetto della vigente normativa nazionale ed europea in materi di trattamento dei dati personali di cui al D.Lgs. n. 196/2003, s.m.i. e al Regolamento dell'Unione Europea n. 679/2016 ovvero in osservanza delle prescrizioni e dei principi ivi contemplati (Principi di necessità, liceità, trasparenza, correttezza e proporzionalità).
Nel dettaglio.

- Il trattamento dei dati deve essere effettuato in modo lecito e corretto.
- I dati personali devono essere trattati unicamente ed esclusivamente per le finalità inerenti alle attività lavorative affidate e di competenza dell'Area _____facente capo alla Direzione _____.
- I dati personali, quindi, devono essere raccolti, registrati e successivamente trattati unicamente per le finalità inerenti all'attività di competenza e/o attività connesse.
- Le modalità con cui si effettuano i trattamenti devono essere pertinenti e non eccedenti le finalità perseguite (ovvero l'incaricato è autorizzato al trattamento dei dati personali al solo fine di effettuare le proprie attività lavorative di competenza).
- Il trattamento dei dati personali deve avvenire solo se necessario allo svolgimento della propria attività lavorativa, escludendo lo stesso quando le finalità perseguite possono essere realizzate mediante l'utilizzo di dati anonimi e/o mediante modalità che permettano di identificare l'interessato solo in caso di necessità (principio di limitazione del trattamento

dei dati).

- I dati personali oggetto di trattamenti devono essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento compatibilmente con i predetti scopi.
- Il trattamento dei dati deve essere effettuato secondo il principio di trasparenza, ovvero deve essere assicurata la consapevolezza dell'interessato in ordine al trattamento dei dati che lo riguardano.
- Se necessario e correlato alle mansioni lavorative svolte, l'incaricato deve verificare costantemente – secondo le istruzioni fornite dal proprio Responsabile – l'esattezza dei dati, il loro aggiornamento e la loro conservazione nel rispetto delle misure/procedure di sicurezza adottate dall'azienda in materia di Privacy, di utilizzo degli strumenti informatici e sicurezza delle informazioni.
- L'incaricato è tenuto ad assicurarsi che i dati trattati non vadano dispersi e/o acquisiti, anche in modo incontrollato, da terzi non autorizzati al trattamento.
- Se necessario e correlato alle mansioni svolte, l'incaricato deve verificare costantemente – secondo le istruzioni fornite dal proprio Responsabile – la completezza e pertinenza dei dati trattati il cui trattamento non deve essere eccedente rispetto alle finalità per le quali sono raccolti e/o successivamente trattati.
- E' vietato modificare i trattamenti esistenti e/o introdurre nuovi trattamenti senza l'esplicita autorizzazione del proprio Responsabile e/o del Direttore _____
- In caso di incidente di sicurezza che coinvolga dati personali (soprattutto dati sensibili) l'incaricato ha l'obbligo prescritto dalla legge di informare tempestivamente il Responsabile dell'Ufficio Privacy e il Responsabile del proprio Ufficio. In particolare, si elencano a titolo esemplificativo e non esaustivo i casi di violazione dei dati personali e/o incidente di sicurezza: distruzione – accidentale e/o illecita – perdita, modifica, divulgazione e accessi non autorizzati ai dati trasmessi, conservati o comunque trattati.
- Devono essere rispettate le indicazioni e/o le istruzioni fornite dal Responsabile dell'Ufficio Privacy e/o dal Responsabile dell'Area _____e/o del Direttore _____. Le operazioni di trattamento devono essere effettuate in osservanza della normativa nazionale ed europea in materia di Privacy nonché nel rispetto delle procedure/regolamenti aziendali adottati dalla LAZIOcrea in materia di trattamento dei dati personali (privacy), utilizzo degli strumenti informatici/elettronici e sicurezza delle informazioni (pubblicati sia sul portale dei dipendenti che sul sito internet nelle apposite sezioni dedicate alla Privacy) e/o misure di sicurezza adottate dalla struttura regionale di riferimento.
- Nel caso in cui devono essere effettuati trattamenti – soprattutto comunicazioni/divulgazioni di dati all'esterno – l'incaricato ha l'obbligo di informare tempestivamente il proprio Responsabile e/o il Direttore al fine di ottemperare agli obblighi relativi alla normativa in materia di Privacy (es obblighi inerenti all'informativa e al consenso).
- In caso di trattamenti che esulano dall'ordinaria gestione ed esecuzione delle attività lavorative affidate (soprattutto comunicazione di dati all'interno degli uffici), l'incaricato ha l'obbligo di informare il proprio Responsabile e/o il Direttore al fine di garantire la corretta osservanza delle prescrizioni di cui alla normativa in materia di Privacy.
- Se correlato alle mansioni lavorative affidate, l'incaricato deve supportare il Responsabile

di Area e/o il Direttore nel garantire agli interessati del trattamento l'esercizio dei diritti contemplati dal Regolamento U.E. 679/2016 nel rispetto delle procedure aziendali adottate (Diritto all'oblio, alla limitazione del trattamento, alla rettifica, all'aggiornamento, alla portabilità dei dati, di opposizione, di non subire profilazione, etc.). Al riguardo si precisa che sarà cura del Responsabile dell'Area/Ufficio di appartenenza e/o del Responsabile dell'Ufficio Privacy fornire ulteriori istruzioni in merito.

- Se correlato alle attività lavorative, l'incaricato deve supportare il Responsabile di Area e/o il Direttore nell'implementazione delle misure tecniche ed organizzative ai fini della corretta osservanza ed attuazione della normativa in materia di Privacy
- Se necessario e correlato all'attività lavorativa svolta, l'incaricato deve procedere all'eventuale cancellazione, limitazione del trattamento, pseudonimizzazione e/o cifratura dei dati nel rispetto delle istruzioni impartite dal proprio Responsabile e/o Direttore in linea con le procedure/regolamenti adottati nonché nel rispetto delle misure di sicurezza prescritte dalla normativa in materia di Privacy.

(Nota: per ulteriori approfondimenti si rinvia ai riferimenti normativi e ai regolamenti/procedure/policy pubblicati sui siti internet e intranet nelle apposite sezioni dedicate alla Privacy)

Obblighi di riservatezza

L'incaricato del trattamento deve garantire la massima riservatezza in relazione ai dati personali trattati e/o di cui venga a conoscenza nell'espletamento delle proprie attività lavorative. L'obbligo di riservatezza deve essere rispettato anche in relazione alle credenziali di autenticazione assegnate (password),
Nel dettaglio l'incaricato deve:

- chiedere l'autorizzazione al Responsabile di Area e/o al Direttore – qualora giungano richieste anche da parte di uffici interni – per effettuare comunicazioni e/o accessi ai dati personali e/o alla documentazione che contiene i dati stessi;
- in caso di interruzione, anche temporanea, delle attività lavorative, adottare tutti gli accorgimenti ritenuti più opportuni al fine di evitare che i dati trattati non siano accessibili a terzi non autorizzati;
- raccogliere, registrare e conservare i dati presenti nei files informatici e/o nei documenti cartacei avendo cura che l'accesso agli stessi sia reso possibile solo al personale autorizzato;
- qualora giungano richieste di comunicazione di dati personali da parte dell'Autorità Giudiziaria e/o degli Organi di Polizia, avvertire comunque il Responsabile dell'Area Privacy e il Responsabile all'Area Privacy di lavoro prima di comunicare i dati stessi;
- fermo restando i divieti di cancellazione e/o obblighi di conservazione stabiliti dalle normative di legge, distruggere o comunque rendere illeggibili i documenti cartacei – che contengono dati personali – non più utilizzati, prima che gli stessi vengano cestinati.

Inoltre è vietato:

- comunicare e/o diffondere dati personali a terzi non autorizzati al trattamento senza l'autorizzazione del proprio Responsabile e/o del Responsabili dell'Area Privacy e, ove

necessario, previo rilascio dell'informativa obbligatoria e/o prestazione del consenso da parte degli interessati al trattamento;

- comunicare dati personali ad un collega autorizzato al trattamento in presenza di terzi non autorizzati;
- parlare ad alta voce quando si comunicano i dati personali (anche per telefono), evitando comunque che terzi non autorizzati vengano a conoscenza di informazioni personali ascoltando la conversazione;
- comunicare ad un collega autorizzato al trattamento e/o ad un terzo non autorizzato le proprie credenziali di autenticazione.

Gli obblighi relativi alla riservatezza dei dati trattati dovranno essere osservati anche a seguito di cambiamento delle mansioni lavorative assegnate (es. mobilità), cessazione del rapporto di lavoro e/o temporanea sospensione delle attività lavorative (es. aspettativa, maternità e/o congedi parentali).
Il trattamento dei dati deve avvenire assicurando la tutela della riservatezza, integrità e disponibilità dei dati stessi, nonché nel rispetto della dignità della persona dell'interessato al trattamento. In particolare le operazioni di trattamento devono essere effettuate eliminando ogni occasione di impropria e/o illegittima conoscibilità di informazioni personali da parte di terzi non autorizzati al trattamento.

Qualora il trattamento dei dati sia effettuato in violazione dei principi sopra menzionati e di quanto disposto dalla normativa in materia di Privacy, l'incaricato ha l'obbligo stabilito dalla normativa stessa di informare tempestivamente il Responsabile dell'Ufficio Privacy e il proprio Responsabile al fine di procedere eventualmente al blocco dei dati trattati (vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del trattamento medesimo) e/o consentire l'osservanza degli obblighi di legge relativi alle notifiche al Garante Privacy (data breach).

Obblighi inerenti al trattamento con l'ausilio di strumenti elettronici

Le istruzioni di seguito riportate sono vincolanti per il personale dipendente se correlate alle attività lavorative assegnate.

In base a quanto stabilito dalla normativa vigente in materia di Privacy sia nazionale – art. 33, 34 e 36 D.Lgs. 196/2003 e Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B stesso decreto) – che europea – Regolamento Europeo n. 679/2016 – per le operazioni di trattamento dei dati personali effettuate con strumenti elettronici/automatizzati, l'incaricato del trattamento deve osservare le misure di sicurezza adottate dall'Azienda e specificate nei relativi regolamenti e/o procedure in materia di Privacy, in materia di utilizzo di strumenti informatici, internet e posta elettronica nonchè in materia di sicurezza delle informazioni (ISO 27001) pubblicati sui siti internet e intranet nelle apposite sezioni (sezioni dedicate alla Privacy e sezioni dedicate alle procedure/MOG/Qualità, etc.).

Nel dettaglio si riportano di seguito gli obblighi inerenti all'utilizzo delle credenziali di autenticazione (UserID e Password).

L'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente riservata delle proprie credenziali di autenticazione (password) nonché la diligente custodia dei dispositivi elettronici (computer) in uso esclusivo e/o comunque in possesso dell'incaricato.
Nel dettaglio risulta necessario:

- Elaborare la password secondo le indicazioni fornite e riportate nei regolamenti/procedure aziendali e conservare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (username).
- Rispettare i profili di autorizzazione attribuiti ai fini dell'accesso ai dati e ai sistemi (ovvero all'utilizzo di determinati applicativi informatici e/o piattaforme informatiche nell'ambito delle attività lavorative assegnate).
- Custodire in modo diligente i dispositivi elettronici in possesso e/o in uso esclusivo.

Inoltre, si precisa quanto segue:

- La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri, di cui almeno quatto devono essere di natura numerica.
- Risulta necessario che la parola chiave non contenga riferimenti agevolmente riconducibili all'incaricato; quindi, la parola chiave non deve essere: il nome o il cognome dell'incaricato, il soprannome, la data di nascita propria, dei figli o degli amici, il nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi, il nome e cognome di personaggi famosi, etc.

E' vietato:

- rivelare la parola chiave a terzi non autorizzati;
- scrivere la parola chiave in un messaggio di posta elettronica;
- rivelare la parola chiave al superiore;
- dare indicazione in merito al formato ed alla lunghezza della parola chiave;
- svelare la parola chiave su questionari e/o su formulari di sicurezza.

La parola chiave deve essere modificata dall'incaricato almeno ogni sei mesi, in caso di trattamento di dati sensibili e/o di dati giudiziari la parola chiave deve essere modificata obbligatoriamente ogni tre mesi. Al riguardo si precisa che il sistema adottato dalla LAZIOcrea prevede in automatico la modifica della parola chiave ogni tre mesi.

Si riportano di seguito ulteriori istruzioni in ordine all'utilizzo di strumenti elettronici.

- ✓ L'incaricato ha l'obbligo di terminare la sessione di lavoro, al computer, ogni volta che si deve allontanare, anche solo per poco tempo, dal proprio ufficio.
- ✓ Spetta all'incaricato mettere in atto gli accorgimenti ritenuti più opportuni affinché anche in sua assenza, il computer non resti incustodito e/o accessibile a terzi non autorizzati.
- ✓ In ogni caso deve essere attivata la funzione screen saver qualora l'incaricato si allontani, anche solo per pochi minuti, dal proprio ufficio.
- ✓ Risulta, inoltre, importante curare la conservazione e la segretezza della parola chiave evitando di trascriverla su supporto cartaceo precario o visibile (es. post-it) oppure di tenerla nel portafoglio o trascritta nella prima pagina dell'agenda o della rubrica di ufficio o in qualunque altro posto facilmente intuibile;

Al fine di tutelare l'integrità dei dati trattati e memorizzati sui files di rete, si precisa che l'azienda ha adottato un sistema di *back up che* opera in automatico a fine giornata lavorativa.
Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Obblighi inerenti ai trattamenti senza l'ausilio di strumenti informatici
Le istruzioni di seguito riportate sono vincolanti per il personale dipendente se correlate all'attività lavorativa assegnata.

Per le operazioni di trattamento dei dati personali effettuate senza l'ausilio di strumenti elettronici, l'incaricato del trattamento deve osservare le misure di sicurezza adottate dalla LAZIOcrea in osservanza di quanto stabilito dalla normativa in materia di Privacy di cui agli articoli 33, 35 e 36 del D.Lgs. 196/2003, di quanto disposto dal Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B stesso Decreto) e dal Regolamento dell'Unione Europea n. 679/2016. In particolare l'incaricato ha l'obbligo di rispettare le procedure e/o i regolamenti aziendali in materia di Privacy, sicurezza delle informazioni e in materia di archivio e protocollo.
Nel dettaglio si elencano di seguito le regole principali che l'incaricato deve osservare nelle operazioni di trattamento dei dati personali.

- I documenti che contengono dati personali non devono essere portati al di fuori dei locali individuati per la loro conservazione, se non in casi del tutto eccezionali, e nel caso questo avvenga, l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le operazioni di trattamento.
- Nel periodo di tempo in cui i documenti che contengono dati personali si trovano al di fuori dei locali individuati per la loro conservazione, l'incaricato del trattamento non deve lasciarli mai incustoditi.
- L'incaricato del trattamento deve inoltre controllare che i documenti che contengono dati personali, composti da numerose pagine o più raccoglitori, siano sempre completi ed integri.
- Al termine dell'orario di lavoro, l'incaricato del trattamento deve riportare tutti i documenti che contengono dati personali nei locali (Archivi) individuati per la loro conservazione.
- I documenti (Faldoni, Raccoglitori, Fascicoli, etc.) che contengono dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.
- Risulta necessario adottare ogni cautela affinché persone non autorizzate non vengano a conoscenza dei dati personali contenuti nei documenti utilizzati per lo svolgimento delle attività lavorative.
- Per evitare il rischio di divulgazione dei dati personali si deve limitare l'utilizzo di copie fotostatiche. Particolare cautela deve essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato.

Risulta inoltre vietato:

- Effettuare copie fotostatiche o di qualsiasi altra natura – non autorizzate dal proprio Responsabile – di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Sottrarre, cancellare, distruggere – senza l'autorizzazione del proprio Responsabile – stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Consegnare – a persone non autorizzate dal Responsabile di Area e/o dal Direttore – stampe, tabulati, elenchi, rubriche e, più in generale, ogni altro materiale che contiene dati/informazioni personali oggetto del trattamento.

In riferimento, invece, agli obblighi inerenti alla sicurezza degli archivi cartacei nonché alla sicurezza nella cancellazione dei dati si elencano le seguenti regole che l'incaricato deve osservare.

Sicurezza Archivi Cartacei

- L'accesso agli Archivi cartacei è limitata al solo personale autorizzato al trattamento e ai soli dati la cui conoscenza sia strettamente necessaria per adempiere alle attività lavorative assegnate.

La chiave degli archivi è fornita ai soli soggetti autorizzati.

Nel caso di dati sensibili e giudiziari, inoltre, devono essere osservate le seguenti regole:

- Le cartelle o fascicoli o supporti cartacei di vario genere che contengono dati personali devono essere conservati in armadi (Archivi) muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro dall'incaricato del trattamento.
- Maggiori cautele devono essere utilizzate per i documenti e/o atti che contengono dati sensibili e giudiziari; in particolare i menzionati dati affidati all'incaricato del trattamento, qualora non vengano utilizzati, devono essere conservati in contenitori chiusi a chiave (es. cassettiere) fino al loro rientro in archivio.

Ai fini della sicurezza degli Archivi cartacei, LAZIOcrea ha adottato dispositivi di sicurezza passiva come rilevatori di fumo, allarme, estintori.

Sicurezza nella cancellazione dei dati

- La cancellazione dei dati personali può essere effettuata – previa autorizzazione del Responsabile di Area e/o del Direttore e/o - quando la conservazione degli stessi non è più necessaria per legge e/o per gli scopi per cui sono stati raccolti e successivamente trattati.
- I dati personali possono essere cancellati anche su richiesta dell'interessato al trattamento (anche ai fini dell'esercizio del diritto all'oblio) - sempre che la conservazione non sia necessaria per legge e/o per la gestione del rapporto di lavoro (e/o contrattuale nel caso di consulenti e/o fornitori) - e comunque previa autorizzazione del Responsabile di Area e/o del Direttore.
- L'eventuale distruzione dei dati deve essere effettuata con sistemi meccanici o

automatizzati in modo da evitare ogni possibile recupero. In caso di cancellazione dei dati memorizzati sui files elettronici, l'incaricato è tenuto al rispetto dei regolamenti/procedure aziendali (es. utilizzo funzione "svuotamento del cestino in modalità sicura") nonché delle istruzioni impartite dal Responsabile di Area e/o dal Direttore.

- I documenti che contengono dati personali forniti all'Azienda per la gestione del rapporto di lavoro e/o per l'esecuzione della propria attività lavorativa e/o per l'esecuzione di contratti con fornitori/consulenti esterni (ivi comprese l'esecuzione delle attività formative del personale dipendente) e/o per l'erogazione di servizi a supporto dell'amministrazione regionale dovranno essere restituiti e/o cancellati – previa autorizzazione del Responsabile di Area e/o del Direttore – alla cessazione del rapporto di lavoro e/o estinzione del rapporto contrattuale e/o comunque in tutti i casi in cui il trattamento dei dati personali non risulta essere più necessario per il perseguimento delle finalità suindicate, salvo diversa prescrizione di legge.

In ogni caso l'incaricato del trattamento ha l'obbligo di controllare e custodire i dati personali oggetto del trattamento in modo da evitare o, comunque, ridurre al minimo i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.

L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato dal Responsabile di Area e/o dal Direttore. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate su istruzione del Responsabile. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate dal Responsabile di Area.

Per quanto non previsto nel presente atto, si precisa che sarà cura del Responsabile dell'Ufficio Privacy e/o del Responsabile di Area e/o del Direttore fornire ogni altra istruzione e/o raccomandazione in ordine alle operazioni di trattamento dei dati personali, alla gestione e custodia degli stessi nel rispetto della vigente normativa in materia di Privacy nonché nel rispetto delle normative applicabili alle diverse tipologie di attività effettuate nei singoli uffici/Aree aziendali (es. normativa in materia di Archivio, in materia di Sicurezza delle informazioni, in materia di Salute e Sicurezza sui luoghi di lavoro, in materia di conservazione di atti e documenti amministrativi, etc.).

La presente nomina si intende valida per tutta la durata delle attività lavorative assegnate e di competenza dell'Area _____. In caso di cessazione del rapporto di lavoro (anche interruzione temporanea delle attività lavorative come ad es. nei casi di aspettativa, congedi parentali, maternità, etc.) e/o cambiamento delle mansioni affidate, è vietato comunicare e/o divulgare dati personali di cui l'incaricato è venuto a conoscenza nell'espletamento delle mansioni lavorative assegnate.

Per ogni altra misura di sicurezza e/o istruzione e/o raccomandazione non contemplate nel presente atto, si rinvia ai Regolamenti/Procedure Aziendali in materia di trattamento dei dati personali pubblicati sul sito internet e sul portale dei dipendenti e/o pubblicati nelle sezioni dedicate ai Fornitori e/o dedicate alla Qualità e/o dedicate alla pubblicazione del Modello Organizzativo di Gestione e Controllo di LAZIOcrea SpA.

Roma,

LAZIOcrea SpA
Presidente e legale rappresentante
Dott. Andrea Umena

Roma,

Per conoscenza e accettazione
Gli incaricati del trattamento
.....
.....

All. n. 2 Atto di Nomina ad "*incarico del trattamento dei dati personali*" in attuazione della normativa nazionale ed europea in materia di Privacy.

La LAZIOcrea SpA con sede in 00142 Roma, via del Serafico n.107 - - Titolare del trattamento dei dati personali afferenti al proprio personale dipendente, ai consulenti e ai fornitori esterni (ivi compresi i docenti/tutor esterni che effettuano attività formative nell'interesse della società stessa) ai sensi della normativa nazionale e europea in materia di Privacy di cui all'28 D.Lgs.196/2003 e all'art. 4, par. 7) Regolamento UE n. 679/2016 nonché in qualità di Responsabile del Trattamento dei dati personali della Regione Lazio ed Enti collegati ai sensi degli articoli 29 D.Lgs 196/203 e 4, par) 8) e 28 del Regolamento UE. - rappresentata per il presente atto dal Presidente legale rappresentante pro tempore Dott. Umena Andrea domiciliato per la carica presso la suddetta sede aziendale.

VISTO
Il decreto legislativo 30 giugno 2003, n. 196 c.d. "Codice in materia di protezione dei dati personali",

Il Regolamento dell'Unione Europea n. 679/2016.
ed in particolare:
-Il combinato disposto degli articoli 4 comma 1 lett f) e 28 del D.Lgs 196/2003 e degli articoli 4, par.7 e 26 Regolamento UE 679/2016 che definiscono il Titolare del trattamento come la persona fisica, la persona giuridica, la pubblica amministrazione, o qualsiasi altro ente, associazione od organismo anche periferico cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
-Il combinato disposto degli articoli 29, comma 5 D.Lgs 196/2003 e 28 Regolamento UE 679/2016 che prevedono "Il Responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni";
-L'art. 4, comma 1, lett. h) D.Lgs 196/2003 che definisce la figura degli incaricati come "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".
-L'art. 30 D.Lgs 196/2003 che prescrive al comma 1. "le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile attenendosi alle istruzioni impartite"; al comma 2 "la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima".

- Il combinato disposto articoli 4 parag. 10 e art. 29 Regolamento UE 679/2016 che individuano la figura degli autorizzati al trattamento sotto l'autorità diretta del Titolare e/o del Responsabile del trattamento, ossia coloro che devono essere istruiti in tal senso (figura riconducibile a quella dell'incaricato del trattamento prevista specificatamente dalla normativa nazionale sulla Privacy di cui al suindicato art. 30)

CONSIDERATO

-che la Regione Lazio è Titolare del trattamento dei dati personali afferenti ai cittadini/utenti dell'amministrazione stessa ai fini dell'esercizio delle proprie competenze istituzionali – esercitate sia mediante le proprie strutture amministrative che congiuntamente ad altri Enti e/o Soggetti Pubblici in situazione di contitolarità del trattamento secondo il disposto normativo di cui all'art. 26 regolamento UE 679/2016 - , nonché dei dati relativi al proprio personale dipendente ivi compresi i soggetti con funzione apicali e politiche, i fornitori e i consulenti esterni;

-che la LAZIOcrea S.p.A. svolge attività connesse all'esercizio delle funzioni amministrative della Regione Lazio di cui all' art. 118 della Costituzione, oltre alle attività di progettazione, realizzazione e gestione della strategia regionale di Agenda Digitale, incluso il Sistema Informativo Regionale, nonché di Organismo Intermedio e/o di soggetto attuatore di interventi co-finanziati dall'Unione Europea e di Centrale di Committenza, previa autorizzazione dell'Amministrazione Regionale;

-che la LAZIOcrea, quindi, conformemente allo Statuto e sulla base di quanto stabilito e disciplinato dal Contratto Quadro sottoscritto in data 29.12.2017, eroga servizi e realizza i progetti per la Regione Lazio sulla base dei fabbisogni espressi dalle diverse strutture regionali;

-che la Giunta Regionale, su proposta della Direzione regionale Centrale Acquisti, entro il 31 dicembre dell'anno precedente a quello di riferimento, approva il Piano Operativo Annuale (POA), corredato del relativo parere di congruità di cui all'art. 192 del D. Lgs. n° 50/2016, contenente la pianificazione dettagliata delle attività affidate alla LAZIOcrea, articolato in macroaree e servizi;

-che i menzionati servizi svolti dal personale dipendente della LAZIOcrea comportano un continuo trattamento di dati personali (generici, sensibili e giudiziari) rientranti nella sfera di titolarità dell'amministrazione regionale ai sensi del suindicato art. 28 del Codice, e quindi rientrano nell'ambito di applicazione della normativa in materia di Privacy;

- che, dunque, la Regione Lazio, secondo quanto prescritto dall'art. 29 D.Lgs 196/2003, ha designato il legale rappresentante pro-tempore della LAZIOcrea Responsabile esterno del trattamento dei dati personali – rientranti nella sfera di titolarità dell'amministrazione stessa – con Deliberazione di Giunta Regionale 797 del 29.11.2017.

-che, inoltre, in osservanza del Regolamento Europeo sulla Privacy il Titolare e/o il Responsabile del trattamento deve garantire la riservatezza dei dati trattati, quindi gli addetti al trattamento (personale incaricato con il presente atto) sono obbligati al rispetto dei relativi obblighi (riportati di seguito) nonché delle istruzioni impartite dal Titolare stesso e/o Responsabile stesso (riportate di seguito).

RITENUTO

pertanto, di dover procedere - in attuazione di quanto prescritto dalla suindicata normativa in materia di Privacy - alla nomina ad "incaricato del trattamento dei dati personali" del personale dipendente della LAZIOcrea che svolge attività inerenti al servizio/progetto _____(indicare servizio così come denominato nel POA) a supporto _____(indicare la Struttura Regionale di riferimento del servizio: es Direzione e/o

Agenzia e/o struttura facente capo ad altra struttura es Presidenza) (servizio specificato nel POA - Macroarea _____).

NOMINA

per quanto in premessa
ai sensi e per gli effetti dell'art. 30 D.Lgs 196/2003, i sottoscrittori del presente atto – dipendenti della LAZIOcrea SpA – "Incaricati del trattamento dei dati personali" - effettuato nell'ambito delle attività di competenza _____(indicare la struttura regionale di riferimento come sopra) al fine di consentire il lecito svolgimento delle operazioni di trattamento dei dati personali correlate alla corretta esecuzione del servizio assegnato e inerente alle attività connesse all'esercizio delle funzioni amministrative di competenza della menzionata struttura amministrativa meglio specificate nel POA (indicare il capitolo/scheda tecnica del POA afferente al servizio) vigente secondo le modalità di seguito indicate.

La presente nomina è da intendersi valida solo per le tipologie di trattamento – tra quelle contemplate dall'art. 4 lett. A) del D.Lgs 196/2003 e dall'art. 4 paragr. 2) Regolamento Europeo – necessarie ai fini dell'effettuazione del servizio richiesto e secondo le modalità e le istruzioni riportate nel presente atto e impartite dal Titolare del trattamento anche a mezzo del Responsabile della struttura regionale di riferimento.

In particolare gli incaricati designati con il presente atto possono effettuare solo quelle tipologie di trattamento – ovvero operazioni o complesso di operazioni svolte sui dati con o senza l'ausilio di strumenti elettronici/automatizzati– espressamente autorizzate e richieste dai Responsabili interni della struttura regionale di riferimento, e possono accedere ai data base, ai sistemi informativi e/o agli applicativi informatici solo previa autorizzazione (del Direttore Regionale Responsabile) e creazione dell'utenza da parte della competente struttura e/o del Responsabile dei Sistemi informativi dell'amministrazione regionale.

A tal fine si forniscono di seguito istruzioni e raccomandazioni in ordine alla corretta effettuazione delle operazioni di trattamento dei dati della Regione Lazio in osservanza della normativa in materia di Privacy e degli standard relativi alla sicurezza delle informazioni (UNI CEI ISO/IEC 27001).

Istruzioni in ordine alle modalità con cui devono essere effettuate le operazioni di trattamento dei dati personali della Regione Lazio (_____indicare la struttura regionale/Direzione competente)
Le istruzioni di seguito riportate sono vincolanti per il personale dipendente se correlate all'attività lavorativa assegnata.

Le operazione di trattamento dei dati personali devono essere effettuate nel rispetto della vigente normativa nazionale ed europea in materi di trattamento dei dati personali di cui al D.Lgs. n. 196/2003, s.m.i. e al Regolamento dell'Unione Europea n. 679/2016 ovvero in osservanza delle prescrizioni e dei principi ivi contemplati ovvero dei principi di necessità, liceità, trasparenza, correttezza e proporzionalità.
Nel dettaglio.

- Il trattamento dei dati deve essere effettuato in modo lecito (rispetto delle disposizioni normative applicabili) corretto e trasparente secondo quanto prescritto dagli articoli 5, 6, 7 e 12 del Regolamento UE 679/2016 nonché in osservanza dei diritti di cui all'informativa e ai diritti di accesso ai dati, limitazione del trattamento, cancellazione e rettifica di cui agli articoli 12, 13, 14,15, 16,17 e 18 del Regolamento stesso.
- I dati personali devono essere trattati unicamente per le finalità inerenti al servizio svolto a supporto della struttura regionale di riferimento (specificato nel POA vigente) e attività connesse.
- Le modalità con cui devono essere svolte le operazioni di trattamento devono essere pertinenti e non eccedenti le finalità perseguite, ovvero l'incaricato è autorizzato al trattamento dei dati personali al solo fine di effettuare il servizio richiesto correlato alle finalità istituzionali perseguite dalla struttura regionale di riferimento.
- Il trattamento dei dati personali deve avvenire solo se necessario allo svolgimento della propria attività lavorativa, escludendo lo stesso quando le finalità perseguite possono essere realizzate mediante l'utilizzo di dati anonimi e/o mediante modalità che non permettano di identificare l'interessato (se non in caso di necessità e secondo i termini e le condizioni prescritte dalla normativa vigente).
- I dati personali oggetto di trattamenti devono essere trattati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento compatibilmente con i predetti scopi.
- Il trattamento dei dati deve essere effettuato secondo il principio di trasparenza, ovvero deve essere assicurata la consapevolezza dell'interessato in ordine al trattamento dei dati che lo riguardano, e deve fornire, se correlato alle attività lavorative svolte, l'informativa agli interessati e/o richiedere il consenso quando previsto dalla vigente normativa in materia di Privacy.
- Se necessario e su autorizzazione della struttura regionale competente, l'incaricato deve verificare l'esattezza dei dati e il loro aggiornamento e garantirne la corretta conservazione nel rispetto delle misure/procedure di sicurezza adottate dall'amministrazione regionale/struttura di riferimento e in osservanza delle istruzioni impartite caso per caso dai Responsabili dell'amministrazione stessa.
- L'incaricato è tenuto ad assicurarsi che i dati trattati non vadano dispersi e/o acquisiti, anche in modo incontrollato, da terzi non autorizzati al trattamento.
- Se necessario e correlato alle attività lavorative svolte, l'incaricato deve verificare costante la completezza e pertinenza dei dati trattati il cui trattamento non deve essere eccedente rispetto alle finalità per le quali sono stati raccolti e successivamente trattati nell'ambito della struttura regionale di riferimento.
- Inoltre è vietato modificare i trattamenti esistenti e/o introdurre nuovi trattamenti senza l'esplicita autorizzazione scritta del Responsabile dell'amministrazione regionale di riferimento.
- In caso di incidente di sicurezza che coinvolga dati personali (violazione della sicurezza e riservatezza dei dati personali) - ovvero qualsiasi situazione che possa comportare una violazione così come definita dall'art. 4, paragrafo 12 del Regolamento n. 678/2016 - l'incaricato ha l'obbligo prescritto dalla legge di informare tempestivamente il Titolare del trattamento, il Responsabile della struttura regionale di riferimento e il coordinatore del

progetto a cui l'incaricato stesso è stato assegnato.

- Qualora giungano richieste di comunicazione di dati personali da parte dell'Autorità Giudiziaria e/o degli Organi di Polizia avvertire comunque il Responsabile della struttura regionale di riferimento e il Coordinatore del progetto prima di comunicare i dati stessi
- Devono essere rispettate le misure di sicurezza riportate nei regolamenti/procedure adottate dall'amministrazione regionale di riferimento in materia di trattamento dei dati personali, utilizzo dei mezzi informatici e sicurezza delle informazioni nonché le indicazioni e/o istruzioni fornite dal Titolare del Trattamento dei dati per mezzo del Dirigente Responsabile della struttura di riferimento.
- Devono essere rispettate le misure di sicurezza riportate nei regolamenti/procedure adottate dalla LAZIOcrea - con particolare riferimento al codice comportamentale per il personale dipendente – nonché le istruzioni riportate nel presente documento e impartite dal Responsabile della struttura regionale di riferimento e/o dal Responsabile/Coordinatore del progetto aziendale di riferimento.
- Più in generale, le operazioni di trattamento dei dati personali devono essere effettuate in osservanza della normativa nazionale ed europea in materia di Privacy, degli standard ISO 27001 in materia di sicurezza delle informazioni, e delle disposizioni normative applicabili secondo le istruzioni del Responsabile della struttura amministrativa di riferimento.

Obblighi di riservatezza

L'incaricato del trattamento deve garantire la massima riservatezza in relazione ai dati personali trattati (soprattutto sensibili e giudiziari) e/o di cui venga a conoscenza nell'espletamento delle proprie attività lavorative nonché, più in generale, di tutte le informazioni acquisite.
L'obbligo di riservatezza deve essere rispettato anche in relazione alle credenziali di autenticazione (userid – password) assegnate.
Nel dettaglio è vietato:

- comunicare e/o diffondere dati personali a terzi non autorizzati al trattamento senza l'autorizzazione del Titolare del trattamento anche per mezzo dei Responsabili delle strutture amministrative regionali di riferimento e/o – ove prescritto dalla vigente normativa – senza previo rilascio dell'informativa obbligatoria e/o prestazione del consenso da parte degli interessati al trattamento.
- Fornire i dati qualora giungano richiesta telefoniche - o anche attraverso altra forma di comunicazione - che non consentano l'identificazione certa del soggetto richiedente.
- comunicare dati personali ad un collega autorizzato al trattamento in presenza di terzi non autorizzati.
- parlare ad alta voce quando si comunicano i dati personali (anche per telefono), evitando comunque che terzi non autorizzati vengano a conoscenza di informazioni personali ascoltando la conversazione.
- Comunicare ad un collega autorizzato al trattamento e/o ad un terzo non autorizzato le proprie credenziali di autenticazione.

Inoltre

- L'accesso ai dati e il relativo trattamento dovrà essere limitato all'espletamento delle proprie attività lavorative ed esclusivamente negli orari di lavoro.

- In caso di interruzione, anche temporanea, delle attività lavative risulta necessario verificare che i dati trattati non siano accessibili a terzi non autorizzati.
- Risulta necessario raccogliere, registrare e conservare i dati presenti nei files informatici e nei documenti cartacei avendo cura che l'accesso agli stessi sia reso possibile solo al personale autorizzato.
- Risulta necessario distruggere o comunque rendere illeggibili – anche mediante apposita attrezzatura - i documenti cartacei che contengono dati personali prima che gli stessi vengano cestinati.

Gli obblighi di cui sopra, relativi alla riservatezza dei dati trattati, ovvero dei dati/informazioni personali di cui l'incaricato è venuto a conoscenza per ragioni di lavoro, dovranno essere osservati anche a seguito di cambiamento delle mansioni lavorative assegnate (es. mobilità), cessazione del rapporto di lavoro e/o temporanea sospensione delle attività lavorative (es. aspettativa, maternità e/o congedi parentali) e/o cessazione del servizio richiesto dall'amministrazione regionale.
Il trattamento dei dati deve avvenire assicurando la tutela della riservatezza, dell'integrità e della disponibilità dei dati stessi, nonché nel rispetto della dignità della persona dell'interessato al trattamento. In particolare le operazioni di trattamento devono essere effettuate eliminando ogni occasione di impropria e/o illegittima conoscibilità di informazioni personali da parte di terzi non autorizzati al trattamento.

Qualora il trattamento dei dati sia effettuato in violazione dei principi sopra menzionati e di quanto disposto dalla normativa in materia di protezione dei dati personali, l'incaricato ha l'obbligo di informare il Responsabile della struttura regionale di riferimento al fine di procedere, se necessario, al blocco dei dati trattati, vale a dire alla sospensione temporanea di ogni operazione di trattamento, fino alla regolarizzazione del trattamento medesimo e/o consentire l'osservanza degli obblighi di legge relativi alle notifiche all'Autorità Garante della Privacy (data breach).

Obblighi inerenti al trattamento dei dati personali con l'ausilio di strumenti elettronici
Le istruzioni di seguito riportate sono vincolanti per il personale dipendente se correlate all'attività lavorativa assegnata.

In base a quanto stabilito dalla normativa vigente in materia di Privacy sia nazionale – art. 33, 34 e 36 D.Lgs. 196/2003 e Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B stesso decreto) – che europea – Regolamento Europeo n. 679/2016 - per le operazioni di trattamento dei dati personali effettuate con strumenti elettronici/automatizzati, l'incaricato del trattamento deve osservare le misure di sicurezza adottate dall'amministrazione regionale e specificate nei relativi regolamenti e/o procedure in materia di Privacy, in materia di utilizzo di strumenti informatici, internet e posta elettronica nonché in materia di sicurezza delle informazioni (ISO 27001).
In particolare si elencano di seguito gli obblighi inerenti alle credenziali di autenticazione (password) assegnate dall'amministrazione regionale di riferimento.
(Le utenze sono create su autorizzazione del Titolare del trattamento per mezzo del Direttore e/o Dirigente Responsabile della struttura regionale di riferimento)
L'incaricato deve adottare le necessarie cautele per assicurare la segretezza della componente

riservata delle proprie credenziali di autenticazione (password) nonché la diligente custodia dei dispositivi elettronici (computer) in uso esclusivo e/o comunque in possesso dell'incaricato.

Nel dettaglio risulta necessario:

- Elaborare la password secondo le indicazioni fornite dal Titolare del trattamento anche per mezzo del Dirigente Responsabile della struttura regionale competente e rispettare la segretezza sulla stessa e sulle altre componenti riservate della credenziale di autenticazione (username).
- Rispettare i profili di autorizzazione attribuiti dall'amministrazione regionale competente ai fini dell'accesso ai dati e ai sistemi ovvero all'utilizzo di determinati applicativi informatici e/o piattaforme informatiche nell'ambito delle attività lavorative assegnate.
- Custodire in modo diligente i dispositivi elettronici in possesso e/o in uso esclusivo.

Al riguardo si precisa quanto segue:

- La password (parola chiave), quando è prevista dal sistema di autenticazione, è composta generalmente da almeno otto caratteri, di cui almeno quatto devono essere di natura numerica.
- Risulta necessario che la parola chiave non contenga riferimenti agevolmente riconducibili all'incaricato; quindi, la parola chiave non deve essere: il nome o il cognome dell'incaricato, il soprannome, la data di nascita propria, dei figli o degli amici, il nome di un hobby o di una passione conosciuta o facilmente conoscibile dai colleghi, il nome e cognome di personaggi famosi, etc.
- Inoltre è vietato:
  - rivelare la password (parola chiave) a terzi non autorizzati;
  - scrivere la password (parola chiave) in un messaggio di posta elettronica;
  - rivelare la password (parola chiave) al superiore;
  - dare indicazione in merito al formato ed alla lunghezza della password (parola chiave);
  - svelare la password (parola chiave) su questionari e/o su formulari di sicurezza,
- La password (parola chiave) deve essere modificata dall'incaricato entro il termine stabilito all'interno della struttura regionale di riferimento (i sistemi prevedono in automatico la modifica della parola chiave almeno ogni 6 mesi, in caso di trattamento di dati sensibili e/o giudiziari i sistemi prevedono detta modifica ogni tre mesi).
- L'incaricato ha l'obbligo di terminare la sessione di lavoro, al computer, ogni volta che si deve allontanare, anche solo per poco tempo, dal proprio ufficio; in ogni caso deve essere attivata la funzione screen saver qualora l'incaricato si allontani, anche solo per pochi minuti, dal proprio ufficio.
- Spetta all'incaricato mettere in atto gli accorgimenti ritenuti più opportuni affinché anche in sua assenza, il computer non resti incustodito e/o accessibile a terzi non autorizzati.
- Risulta, inoltre, importante curare la conservazione e la segretezza della password (parola chiave) evitando di trascriverla su supporto cartaceo precario o visibile (es. post-it) oppure di tenerla nel portafoglio o trascritta nella prima pagina dell'agenda o della rubrica di ufficio o in qualunque altro posto facilmente intuibile;
- Al fine di tutelare l'integrità e la disponibilità dei dati trattati e memorizzati sui files di rete, utilizzare i sistemi di back up adottati dalla struttura amministrativa di riferimento secondo le istruzioni fornite dai responsabili della struttura stessa.

Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Obblighi inerenti ai trattamenti senza l'ausilio di strumenti informatici.
Le istruzioni di seguito riportate sono vincolanti per il personale dipendente se correlate all'attività lavorativa assegnata.

In base a quanto stabilito dalla normativa vigente in materia di Privacy sia nazionale - artt. 33, 35 e 36 D.Lgs. n. 196/2003 e del Disciplinare Tecnico in materia di misure minime di sicurezza (Allegato B al D. Lgs. n. 196 del 30 giugno 2003) –che europea - Regolamento Europeo n. 679/2016 - per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici - l'incaricato del trattamento deve osservare le misure minime di sicurezza adottate dall'amministrazione regionale di riferimento e specificate nei relativi regolamenti/procedure in materia di Privacy e di sicurezza delle informazioni (ISO 27001). Inoltre l'incaricato ha l'obbligo di rispettare le procedure e/o i regolamenti dell'amministrazione stessa in ordine alla custodia di atti e documenti amministrativi affidati per lo svolgimento delle attività lavorative, alla conservazione di determinati documenti in archivi ad accesso selezionato e alle modalità di accesso agli archivi stessi.

Nel dettaglio si elencano di seguito le regole principali che l'incaricato deve osservare nelle operazioni di trattamento dei dati personali.

- I documenti (con particolare riferimento ai documenti amministrativi) che contengono dati personali non devono essere portati al di fuori dei locali, armadi e cassetti (protetti con serratura) individuati per la loro conservazione, se non in casi del tutto eccezionali e su autorizzazione del Titolare del trattamento per mezzo dei Responsabili delle strutture amministrative regionali di riferimento; l'asportazione deve essere ridotta al tempo minimo necessario per effettuare le necessarie operazioni di trattamento richieste dal Responsabile stesso.
- Nel periodo di tempo in cui i documenti che contengono dati personali si trovano al di fuori dei locali, armadi e cassetti (protetti con serratura), individuati per la loro conservazione, l'incaricato del trattamento non deve lasciarli mai incustoditi.
- L'incaricato del trattamento deve assicurarsi che i documenti che contengono dati personali composti da numerose pagine (o contenuti in fascicoli, faldoni e/o in più raccoglitori) siano sempre completi ed integri al momento di essere riposti nei locali, armadi e cassetti (protetti con serratura) individuati per la loro conservazione.
- Al termine dell'orario di lavoro, l'incaricato del trattamento deve riportare tutti i documenti che contengono dati personali nei locali (archivi regionali), armadi e cassetti (protetti con serratura) individuati per la loro conservazione.
- I documenti (Faldoni, Raccoglitori, Fascicoli, etc.) che contengono dati personali non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro.

- Risulta necessario adottare ogni cautela affinché persone non autorizzate non vengano a conoscenza dei dati personali e delle informazioni contenuti nei documenti utilizzati per lo svolgimento delle attività lavorative.
- Per evitare il rischio di divulgazione dei dati personali si deve limitare l'utilizzo di copie fotostatiche. Particolare cautela deve essere adottata quando i documenti sono consegnati in originale ad un altro incaricato debitamente autorizzato;

Inoltre è vietato:

- Effettuare copie fotostatiche o di qualsiasi altra natura - non autorizzate dal Titolare del trattamento, anche per mezzo del Dirigente Responsabile della struttura regionale di riferimento, dei dati personali e/o dal Responsabile della struttura regionale di riferimento - di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Sottrarre, cancellare, distruggere - senza l'autorizzazione del Titolare del trattamento, anche per mezzo del Dirigente Responsabile della struttura regionale di riferimento - stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati personali oggetto del trattamento.
- Consegnare a persone non autorizzate dal Titolare del trattamento, anche per mezzo del Dirigente Responsabile della struttura regionale di riferimento stampe, tabulati, elenchi, rubriche e, più in generale, ogni altro materiale che contiene dati/informazioni personali oggetto del trattamento.

In riferimento, invece, agli obblighi inerenti alla sicurezza degli archivi cartacei nonché alla sicurezza nella cancellazione dei dati si elencano le seguenti regole che l'incaricato deve osservare.

Sicurezza Archivi Cartacei

- L'accesso agli archivi cartacei è limitata al solo personale autorizzato al trattamento dal Titolare del trattamento anche per mezzo del Responsabile della struttura regionale di riferimento e ai soli dati la cui conoscenza sia strettamente necessaria per adempiere al servizio richiesto.
- Il personale LAZIOcrea deve essere autorizzato all'accesso agli archivi regionali specificatamente individuati dal Titolare del trattamento e/o dal Responsabile della struttura regionale di riferimento anche attraverso l'utilizzo di apposito registro di accesso; in particolare, su istruzione del Responsabile della struttura/ufficio regionale, devono essere registrate – in apposito registro - tutte le richieste di documentazione indicando: - il nominativo dell'incaricato e/o la struttura che inoltra la richiesta; - la data e l'ora della richiesta ovvero dell'asportazione dei documenti; i documenti e/o le pratiche di cui si richiede l'asportazione dall'archivio; - la data e l'ora della riconsegna dei documenti asportati; - il nominativo dell'incaricato e/o la struttura che ha riconsegnato i documenti; - se necessario la motivazione di un eventuale ritardo nella consegna.
- L'incaricato del trattamento deve osservare eventuali procedure adottate dalla struttura regionale di riferimento in materia di accesso agli archivi selezionato nonché in materia di Privacy e sicurezza delle informazioni.
- Le cartelle o fascicoli o supporti cartacei di vario genere che contengono dati personali

devono essere conservati in locali, armadi e cassettiere (archivi) muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro dall'incaricato del trattamento (e/o dal Responsabile regionale che ha il possesso delle chiavi). Le chiavi degli archivi sono eventualmente fornite dai Responsabili dell'amministrazione regionale ai soli soggetti autorizzati.

Nel caso di dati sensibili e giudiziari, inoltre, devono essere osservate le seguenti regole:

- maggiori cautele devono essere utilizzate per i documenti e/o atti che contengono dati sensibili e/o giudiziari; in particolare i menzionati dati affidati all'incaricato del trattamento, qualora non vengano utilizzati, devono essere sempre conservati in contenitori chiusi a chiave (es. cassettiere) fino al loro rientro in archivio.
- i supporti e i documenti che contengono dati sensibili e/o giudiziari devono essere conservati nei predetti contenitori muniti di serratura, separatamente da ogni altro documento.
- Ai fini della sicurezza degli archivi cartacei l'amministrazione regionale e/o la LAZIOcrea hanno adottato dispositivi di sicurezza passiva come rilevatori di fumo, allarme, estintori, pertanto l'incaricato è obbligato a segnalare ogni eventuale disfunzione o anomalia dei menzionati dispositivi.

Sicurezza nella cancellazione dei dati

- La cancellazione dei dati personali può essere effettuata solo su autorizzazione del Titolare del trattamento anche per mezzo del Responsabile della struttura regionale di riferimento e quando la conservazione degli stessi non è più necessaria per legge e/o per gli scopi per cui sono stati raccolti e successivamente trattati.
- I dati personali possono essere cancellati anche su richiesta dell'interessato, sempre che la conservazione non sia necessaria per legge e/o per la gestione del rapporto di lavoro (e/o contrattuale nel caso di consulenti e/o fornitori), sempre previa autorizzazione del Titolare del trattamento anche per mezzo del Responsabile della struttura regionale di riferimento.
- L'eventuale distruzione dei dati, previa autorizzazione, deve essere effettuata in modo da rendere gli stessi illeggibili anche con l'utilizzo di sistemi meccanici in modo da evitare ogni possibile recupero delle informazioni. In caso di cancellazione dei dati memorizzati sui files elettronici, l'incaricato è tenuto al rispetto dei regolamenti/procedure regionali in ordine alla funzione "svuotamento del cestino in modalità sicura".
- I documenti che contengono dati personali degli utenti/cittadini della Regione Lazio ai fini dell'erogazione dei servizi pubblici richiesti (e/o erogazione di finanziamenti pubblici) dovranno essere trattati ed eventualmente cancellati sempre su autorizzazione specifica del Titolare del trattamento anche per mezzo del Responsabile della struttura regionale competente nei casi stabiliti dalle normative di legge applicabili e/o comunque in tutti i casi in cui il trattamento dei predetti dati e la loro conservazione non costituisce un obbligo prescritto dalla legge (rispettare i tempi di conservazione previsti dalla normativa in materia di conservazione di atti e documenti amministrativi).
- Se connesso con le attività lavorative, l'incaricato deve supportare la struttura regionale di riferimento al fine di garantire i diritti contemplati dal Regolamento Europeo sulla Privacy

(articoli 16 e ss.) secondo le istruzioni del Responsabile della struttura stessa. In particolare, tenuto conto delle finalità del trattamento e del contesto operativo, l'incaricato deve collaborare con il Titolare del trattamento e/o con il responsabile della struttura regionale di riferimento al fine di garantire l'esercizio dei menzionati diritti da parte degli interessati al trattamento (cittadini/utenti della Regione Lazio _____indicare i casi di utenti di altre strutture collegate es assistiti/pazienti delle strutture sanitarie) che si elencano di seguito: diritto ad ottenere l'informativa sul trattamento effettuato dal Titolare, diritto di accesso, diritto di rettifica (ossia ottenere la rettifica dei dati inesatti senza ingiustificato ritardo), diritto alla cancellazione/oblio, diritto di limitazione del trattamento, diritto alla portabilità dei dati, diritto di opposizione, diritto a non subire profilazione.(per ulteriori approfondimenti in merito all'esercizio dei diritti dell'interessato si rinvia al relativo testo normativo nonché alle istruzioni fornite dal Responsabile della struttura regionale di riferimento e alle procedure predisposte in materia di privacy)

In ogni caso l'incaricato del trattamento ha l'obbligo di controllare e custodire i dati personali oggetto del trattamento in modo da evitare o, comunque, ridurre al minimo i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato su istruzione del Responsabile della struttura regionale di riferimento. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, devono essere identificate e registrate su istruzione del Responsabile stesso. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate dal Responsabile della struttura regionale di riferimento.
Per quanto non previsto nel presente atto di nomina, si precisa che sarà cura del Titolare del trattamento, anche per mezzo del Responsabile della struttura regionale di riferimento, fornire ogni altra istruzione e/o raccomandazione in ordine alle operazioni di trattamento dei dati personali, alla gestione e custodia degli stessi nel rispetto della vigente normativa in materia di Privacy e di sicurezza delle informazioni (ISO 27001) nonché nel rispetto delle normative di settore applicabili (es. normativa in materia di Archivio, in materia di Salute e Sicurezza sui luoghi di lavoro, in materia di atti e documenti amministrativi, in materia di digitalizzazione/informatizzazione degli atti e documenti amministrativi, etc.).

La presente nomina si intende valida per tutta la durata delle attività lavorative assegnate e inerenti al servizio erogato dalla LAZIOcrea a supporto dell'amministrazione regionale (_____indicare la struttura regionale competente del servizio specificato nel POA). In caso di cessazione del servizio richiesto e/o cessazione/sospensione del rapporto di lavoro (anche interruzione temporanea delle attività lavorative come ad es. nei casi di aspettativa, congedi parentali, maternità, etc.) e/o modifica delle attività lavorative assegnate (es. mobilità), è vietato comunicare e/o diffondere dati personali di cui l'incaricato è venuto a conoscenza nello svolgimento delle proprie mansioni lavorative.

Per ogni altra misura di sicurezza e/o istruzione e/o raccomandazione non contemplate nel presente atto, si rinvia ai regolamenti/procedure adottate dall'amministrazione regionale di riferimento in materia di trattamento dei dati personali e di sicurezza delle informazioni.

***

Istruzioni specifiche in ordine alla tipologia del servizio affidato alla LAZIOcrea SpA, quindi in ordine alle attività effettuate dal personale dipendente della stessa nell'ambito del servizio _____(specificato nel POA - macroarea _____.)

Le operazioni di trattamento riguardano principalmente le seguenti categorie di dati personali: generici e giudiziari. Potrebbero riguardare anche dati sensibili (ossia relativi alla salute). A titolo esemplificativo e non esaustivo l'incaricato è autorizzato al trattamento dei dati personali identificativi (anagrafici), reddituali, fiscali e giudiziari.
(Nota: i dati personali che l'incaricato tratta nello svolgimento del servizio richiesto – progetto ambiente - sono quelli afferenti agli utenti/cittadini della Regione Lazio e/o rappresentanti di Enti pubblici che formulano richieste di finanziamento di contributi pubblici).

L'incaricato deve trattare i dati personali ai quali ha accesso attenendosi alle istruzioni del Responsabile della struttura regionale di riferimento, ed è autorizzato ad effettuare le operazioni di trattamento solo ed esclusivamente per lo svolgimento del servizio richiesto correlato alle finalità istituzionali della Regione Lazio ovvero al perseguimento degli obiettivi della struttura regionale di riferimento.

L'incaricato può accedere ai sistemi informativi e/o applicativi informatici e alle banche dati solo se autorizzato dal Titolare, anche per mezzo del Responsabile della struttura regionale di riferimento, ossia su autorizzazione e creazione dell'utenza e del conseguente profilo di autorizzazione assegnato.
Si elencano di seguito i sistemi informativi, applicativi informatici e le banche dati a cui è consentito l'accesso nel rispetto delle istruzioni impartite dal Titolare del trattamento e/o da Responsabile della struttura regionale di riferimento.

- ✓ _____
- ✓ _____
- ✓ _____

L'incaricato del trattamento, su richiesta e autorizzazione del Titolare del trattamento, anche per mezzo del Responsabile della struttura regionale di riferimento, può comunicare i dati personali trattati nell'esecuzione del servizio richiesto alle seguenti categorie di soggetti:

- ✓ _____
- ✓ _____
- ✓ (es: soggetti pubblici e/o privati_____)

L'incaricato non può comunicare e/o divulgare dati ad altri soggetti pubblici se ciò non è previsto da specifica norma di legge e comunque senza previa autorizzazione del Titolare del trattamento, anche per mezzo del Responsabile della struttura regionale di riferimento.

L'incaricato è autorizzato all'accesso ai sopra menzionati sistemi e banche dati per l'effettuazione

delle seguenti operazioni e con i limiti di seguito riportati:

- ✓ _____
- ✓ _____
- ✓ (es: acquisizione di dati e informazioni per l'istruttoria tecnico-amministrativa inerente a _____)
- ✓ (es: consultazione ed acquisizione di dati per la gestione delle procedure di _____)

Il trattamento dei dati personali per mezzo dei suindicati sistemi e banche dati esclude comunque qualsiasi operazione che non sia autorizzata dal Titolare e/o dal Dirigente Responsabile della struttura regionale di riferimento e che non sia strettamente funzionale all'esecuzione del servizio richiesto (POA) sempre nei limiti stabiliti dalle normative di legge vigenti e dai regolamenti.

Si riportano di seguito le categorie di trattamento effettuate dagli incaricati nominati con il presente atto tra quelle contemplate dall'art. 4, comma 1, paragrafo 2) del Regolamento U.E. 679/2016.

(Nota: definizione normativa di trattamento di cui all'art. 4 pargraf) 2. : qualsiasi operazioni e/o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, consistenti in: 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, la cancellazione).

(Riportare di seguito le categorie di trattamento effettuate - ossia descrizione generica delle attività – macroattività - svolte dalle risorse assegnate al servizio che comportano un trattamento di dati personali:

- _____
- _____

***

Per quanto non previsto nel presente atto sarà cura del Titolare del trattamento, anche per mezzo del Dirigente Responsabile della struttura regionale di riferimento, fornire ulteriori istruzioni in ordine al corretto svolgimento del servizio richiesto (vedi POA: servizio/progetto_)

Roma,

LAZIOcrea SpA
Presidente e legale rappresentante
Dott. Andrea Umena

Roma,

Per conoscenza e accettazione
Gli incaricati del trattamento

.....

.....

A