Consiglio Regionale della Campania

X LEGISLATURA

UFFICIO DI PRESIDENZA

SEDUTA DEL 1 LUGLIO 2020

Delibera n. 240

L'anno duemilaventi, il giorno 1 (uno) del mese di luglio alle ore 14:00 nella sala riunioni della propria sede al Centro Direzionale di Napoli, isola F13, si è riunito l'Ufficio di Presidenza del Consiglio Regionale, così costituito:

ROSA	D'AMELIO	Presidente
TOMMASO	CASILLO	Vice Presidente
ERMANNO	RUSSO	Vice Presidente
ANTONIO	MARCIANO	Consigliere Questore
MASSIMO	GRIMALDI	Consigliere Questore
VINCENZO	MARAIO	Consigliere Segretario
FLORA	BENEDUCE	Consigliere Segretario

Oggetto: **Adozione del Modello Organizzativo in materia di protezione dei dati (DPMS) del Consiglio Regionale della Campania**

Sono assenti: ///////

Presiede: Dott.ssa Rosa D'Amelio

Assiste il Segretario Generale Santa Brancati

Relatore: Presidente Rosa D'Amelio

Premesso:

- che il Parlamento europeo ed il Consiglio in data 27.04.2016 hanno approvato il Regolamento UE 679/2016 (GDPR - General Data Protection Regulation) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;
- che il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4.05.2016, è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25.05.2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma di legislazione applicativa o attuativa da parte degli stati membri;
- che il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, debbono tenere presenti dal 25.05.2018, data della piena applicazione del Regolamento;
- che ai sensi dell'art.13 della Legge n.163/2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del 27.04.2016 di che trattasi;
- che in data 04.09.2018 è stato pubblicato in G.U. il D. Lgs. 10.08.2018 n.101 di adeguamento del Codice privacy italiano al GDPR, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27.04.2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), con entrata in vigore il 19.09.2018.

Rilevato:

- che le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Titolari del trattamento dei dati personali devono, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy;
- che appare necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questa Amministrazione di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;
- che il Consiglio Regionale della Campania tratta numerose informazioni personali, per tali intendendosi ai sensi di legge tutti i dati riferibili "a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale";
- che la progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dal Personal Computer, nonché l'obbligo di fornire servizi digitali al cittadino (come da Codice dell'Amministrazione Digitale) espone il Consiglio Regionale della Campania ai rischi di un coinvolgimento sia patrimoniale sia penale;
- che l'utilizzo delle risorse informatiche e telematiche del Consiglio Regionale della Campania deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro;

- che il Garante per la protezione dei dati personali (ora "Autorità di controllo"), con un provvedimento generale del 1.03.2007 intitolato "Linee guida del Garante per posta elettronica e internet" ha fornito concrete indicazioni in ordine all'uso dei computer sul luogo di lavoro - in particolare, il provvedimento raccomanda l'adozione, da parte delle organizzazioni, di un disciplinare interno (denominato anche Policy o Regolamento informatico), definito coinvolgendo anche le rappresentanze sindacali, nel quale siano chiaramente indicate le regole per l'uso di Internet e della posta elettronica;
- che tra le priorità poste in capo alle PP.AA. il Garante ha evidenziato che appare fondamentale, nell'attuale contesto caratterizzato da una crescente minaccia alla sicurezza dei sistemi informativi, la pronta attuazione delle nuove misure relative alle violazioni dei dati personali, tenendo in particolare considerazione i criteri di attenuazione del rischio indicati dalla disciplina e individuando quanto prima idonee procedure organizzative per dare attuazione alle nuove disposizioni (data breach).

Ritenuto pertanto opportuno:

- procedere alla definizione di una Politica generale (atto di indirizzo e linee guida) che consenta al Consiglio Regionale della Campania di provvedere con immediatezza all'adattamento dell'organizzazione alle disposizioni contenute nel Regolamento UE 2016/679 chiarendo e disciplinando gli aspetti rimessi alla propria autonomia organizzativa e procedimentale;
- prevedere un sistema di adattamento flessibile, graduale e continuativo alle disposizioni in materia, anche tenuto conto dei successivi interventi, sia normativi che dell'autorità di controllo nazionale;
- attivare una serie di norme, restrizioni e controlli per garantire la sicurezza dei sistemi informatici e definire le responsabilità degli utilizzatori delle risorse informatiche;
- adottare un Modello Organizzato (Data Protection Management System - DPMS) finalizzato ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati con gli strumenti cartacei, elettronici ed informatici.
- istituire un Gruppo di lavoro permanente in materia di adattamento alle norme del GDPR, composto da:
  1. Responsabili di Unità Dirigenziale e rappresentanti degli Organismi designati di specifici compiti e funzioni all'interno del Consiglio Regionale della Campania in relazione alla competenza, preparazione e/o ruolo nel trattamento di categorie particolari di dati;
  2. almeno un Referente ICT interno, quale supporto tecnico per le problematiche di sicurezza tecnologica;
  3. il Responsabile della Protezione dei Dati.
- Il "Gruppo di lavoro GDPR" definisce ed aggiorna in particolare:
  1. un programma permanente di informazione e formazione del personale;
  2. le priorità di intervento per l'adattamento al GDPR;
  3. le misure "adeguate" da adottare per il rispetto della normativa;
  4. la modulistica uniforme, sia ad uso esterno, che ad uso interno (informativa, comunicazioni, nomine, registri, etc.);
  5. l'elenco dei Responsabili esterni del trattamento e dei Designati interni.

Visto:

- il vigente Regolamento sull'ordinamento degli uffici e dei servizi;
- il Dlgs 196/2003 e successive modificazioni ed integrazioni;
- il Dlgs 82/2005 e successive modificazioni ed integrazioni;
- il Regolamento UE 2016/679;

Tutto ciò premesso,

DELIBERA

1) di approvare il documento DPMS 01-001 "**Politica generale per il trattamento dei dati personali**", in attuazione dei principi del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e parte integrante del presente provvedimento;
2) di approvare il documento DPMS 02-001 "**Regolamento per l'utilizzo degli strumenti informatici, posta elettronica e Internet"**, parte integrante del presente provvedimento;
3) di approvare il documento DPMS 03-001 "**Procedura per l'esercizio dei nuovi diritti**" (compreso il Registro delle richieste), parte integrante del presente provvedimento;
4) di approvare il documento DPMS 04-001 "**Gestione della violazione dei dati (Data Breach)"** (compreso i relativi allegati), parte integrante del presente provvedimento;
5) di approvare il documento DPMS 05-001 "**Istruzioni operative per i dipendenti autorizzati a trattare i dati personali**", parte integrante del presente provvedimento;
6) di approvare il documento DPMS 06-001 "**Procedura e modello per la nomina dei Responsabili**" (compreso i modelli di nomina completa e breve, DPMS 06-002 e 06-003 e la "Lista dei responsabili esterni" DPMS 06-004), parte integrante del presente provvedimento;
7) di istituire un gruppo di lavoro permanente in materia di adattamento alle norme del GDPR (**Gruppo di lavoro GDPR)** composto da:
   1. i Designati di Unità Dirigenziale o degli Organismi, incaricati di specifici compiti e funzioni all'interno del Consiglio Regionale della Campania in relazione alla competenza, preparazione e/o ruolo nel trattamento di categorie particolari di dati;
   2. almeno un Referente ICT interno, quale supporto tecnico per le problematiche di sicurezza tecnologica;
   3. il Responsabile della Protezione dei Dati.

Considerata, infine, la continua evoluzione tecnologica e il necessario allineamento normativo, i suddetti testi allegati e approvati con la presente delibera, potranno in futuro essere rivisti, modificati e aggiornati giusto atto di determina del Dirigente della Unità Dirigenziale Sistemi Informativi.

Il Dirigente U.D. Sistemi Informativi
Responsabile della Protezione dei Dati
Giovanna Donadio

Il Direttore Generale Attività Legislativa
Magda Fabbrocini

Il Direttore Generale RFSU ad interim
Santa Brancati

Firmato digitalmente da:Santa Brancati
Limite d'uso:Explicit Text: Questo certificato rispetta le raccomandazioni previste dalla Determinazione Agid N. 121/2019
Data:13/07/2020 18:39:40

Il Segretario Generale
Santa Brancati

Il Consigliere Segretario
Vincenzo Maraio

Firmato digitalmente da:Santa Brancati
Limite d'uso:Explicit Text: Questo certificato rispetta le raccomandazioni previste dalla Determinazione Agid N. 121/2019
Data:13/07/2020 18:40:23

Il Presidente
Rosa D'Amelio

Consiglio Regionale della Campania

Politica generale per il trattamento dei dati personali

Istruzione operativa per l'attuazione dei principi del Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Approvato con _____
del _____ *nr.* _____

Documento	**DPMS 01-001**	**Politica generale per il trattamento e la protezione dei dati personali**

Revisione 1 del 25.05.2020

Premessa

Il Consiglio Regionale della Campania tratta numerose informazioni personali, intendendosi ai sensi di legge tutti i dati riferibili "*a persona fisica identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*" (es. nome, cognome, indirizzi di residenza, e-mail, foto, video, immagini, indirizzi IP, IBAN, dati patrimoniali o reddituali, etc.).

Sotto il profilo qualitativo, oltre a dati personali identificativi c.d. "comuni", si possono rinvenire informazioni di carattere "sensibile", ovvero le categorie particolari di dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché genetici, biometrici e i dati personali idonei a rivelare lo stato di salute e la vita sessuale, nonché i dati personali relativi a condanne penali e reati.

Inoltre, per il trattamento dei dati personali, si utilizzano sia strumenti informatici, sia supporti cartacei o altri supporti di memorizzazione.

Oggetto

Il presente documento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nell'Ente.

Inoltre, il presente documento descrive i ruoli, le responsabilità, le modalità di governo e di gestione operativa in materia di trattamento di dati personali adottati dal Consiglio Regionale della Campania (o dagli Organismi istituiti nell'ambito della propria organizzazione) in qualità di Titolare del trattamento (nel seguito anche "CRC") in ottemperanza al Regolamento (UE) 2016/679 (RGPD).

Campo di applicazione

L'ambito di applicazione del presente documento riguarda CRC, che tratta dati personali sul territorio dello Stato italiano, anche in caso di trasferimento di dati personali da e verso l'estero (Paesi UE ed extra UE).

Destinatari e perimetro

Destinatario della presente Politica è tutto il personale di ogni ordine e grado di CRC, con riguardo alla gestione interna ed esterna dei dati personali. Tutti i soggetti impiegati a vario titolo sono, pertanto, tenuti a seguire i requisiti per il trattamento dei dati personali espressi nella presente Politica.

Regole generali per il trattamento e la protezione dei dati personali

1. Principali definizioni

Nell'allegato 1 "**Glossario e definizioni**" sono riportate le principali definizioni richiamate nel presente documento.

2. Principi generali

CRC si impegna a far rispettare il Regolamento Europeo 2016/679 e, in particolare, i seguenti principi da esso tratti, a tutto il personale e, in alcuni casi, ai fornitori esterni coinvolti nella gestione dei dati personali (Responsabili esterni) del cui trattamento è Titolare.

I dati personali devono essere sempre trattati in modo lecito e secondo correttezza, sempre nel rispetto delle disposizioni di cui al D. Lgs. 30 giugno 2003 n. 196 (e s.m.i.) e del Regolamento UE 2016/679.

L'articolo 5 del Regolamento UE 2016/679 richiede che i dati personali siano:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato ("liceità, correttezza e trasparenza");

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");

d) esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali ("integrità e riservatezza").

Tutti i dipendenti e i collaboratori di CRC, pertanto, sono tenuti a riconoscere se stanno raccogliendo, elaborando, condividendo o utilizzando dati personali. Devono essere consapevoli dei principi generali del Regolamento UE 2016/679 e dei principi che governano la gestione dei dati personali in CRC. Devono inoltre avere chiare le modalità per riferire i problemi relativi al trattamento dei dati personali al Responsabile della Protezione dei Dati nominato.

Tutto il personale che svolge detta attività di trattamento (di seguito indicato come "**il Personale**") è tenuto ad attivarsi per far sì che i dati personali trattati siano sempre esatti e aggiornati.
I trattamenti non devono mai eccedere le finalità per le quali sono stati raccolti.

2.1 Raccolta e utilizzo dei dati

I dati personali devono essere raccolti ed elaborati in modo lecito, corretto e trasparente, e nel rispetto dei principi del Regolamento UE 2016/679.

CRC deve pertanto assicurare che:
- i dati personali vengano raccolti ed utilizzati solo per un giustificato motivo;
- prima della raccolta sia comunicata all'interessato una informativa con le indicazioni su come i suoi dati saranno utilizzati;
- i dati personali vengano utilizzati solo per lo scopo specifico descritto nell'informativa o nel modulo per il consenso;
- sia mantenuto un registro con tutte le informazioni relative alle attività di trattamento svolte.

2.2 Trattare i dati personali in modo lecito, legittimo e trasparente nei confronti dell'interessato

I dati personali devono essere trattati in modo lecito e legittimo rispetto alle finalità specifiche indicate nell'informativa presentata all'interessato (o nel modulo per il consenso, laddove previsto).

Il trattamento dei dati personali non deve violare gli obblighi di legge o di regolamento, il diritto comune o i termini contrattuali sottoscritti con i terzi o le finalità istituzionali perseguite.

Non devono essere trattati dati personali per ulteriori finalità incompatibili con quella iniziale specificata nell'informativa. In caso di utilizzo dei dati personali per una finalità aggiuntiva o diversa da quella originariamente indicata, l'interessato deve essere informato del nuovo trattamento ed eventualmente fornire il suo consenso.

Ogni comunicazione con l'interessato deve essere presentata in un modo chiaro e facilmente comprensibile.

CRC deve garantire che i dati personali raccolti siano adeguati per le finalità previste dell'organizzazione. A tal fine:
- i processi che comportano il trattamento di dati personali e i nuovi sistemi IT che supportano tale trattamento devono essere analizzati prima del trattamento, in modo da assicurare che le informazioni trattate siano pertinenti e non eccessive;

- devono essere previsti controlli periodici relativamente ai processi e ai sistemi IT che trattano dati personali per garantire che il trattamento non ecceda le finalità iniziali previste.

Laddove non è rilevante o necessario elaborare dati personali per gli scopi dell'organizzazione, CRC deve garantire che tali dati personali non vengano trattati.

3. Struttura organizzativa

Le norme sulla protezione dei dati personali individuano alcune figure organizzative obbligatorie:

3.1 Titolare del trattamento

CRC, rappresentato ai fini previsti dal RGPD dal legale rappresentante pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "**Titolare**").

Il Titolare garantisce il rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD. Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non siano stati ottenuti presso lo stesso interessato.

CRC provvede a:

a) nominare eventuali Responsabili esterni del trattamento e i Designati (personale preposto a Unità Dirigenziale o rappresentanti degli Organismi) nelle persone dei funzionari responsabili delle singole strutture o degli Organismi in cui si articola l'organizzazione, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza.

b) nominare il Responsabile della Protezione dei Dati (RPD);

c) nominare quale Responsabile esterno del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto di CRC, relativamente alle banche dati gestite da soggetti esterni a CRC in virtù di convenzioni, di contratti o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

d) decidere, in piena autonomia, in ordine alle finalità e alle modalità dei trattamenti dei dati personali, nonché agli strumenti utilizzati e al profilo della sicurezza;

e) autorizzare e istruire il personale che effettua operazioni di trattamento all'interno di CRC.

CRC favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare.

3.2 Responsabile esterno del trattamento

Nomina dei responsabili esterni

Nei casi in cui un soggetto terzo effettua trattamenti di dati personali per conto di CRC e non può essere considerato come autonomo Titolare, questi è nominato come **Responsabile trattamento dati esterno** ai sensi dell'art. 28 del Regolamento UE 2016/679 (vd. Mod. DPMS 06-001).

Relativamente alla formalizzazione della nomina conseguente a tutte le tipologie di accordi/contratti, ogni Designato di Unità Dirigenziale e ogni rappresentante degli Organismi ha la responsabilità di garantire che tutti i contratti aventi per oggetto in via diretta o indiretta un trattamento dei dati in nome e per conto di CRC contemplino delle specifiche clausole, definite in accordo con il Responsabile della Protezione dei Dati, in cui

si prevede la nomina della controparte a Responsabile esterno del trattamento oggetto del contratto. In alternativa il contratto dovrà essere integrato con l'atto/contratto di designazione a Responsabile Trattamento dei dati esterno.

3.3 Designati al trattamento (delegati)

L'art. 2-quaterdecies ("Attribuzione di funzioni e compiti a soggetti designati") del D.Lgs. 196/2003 (come novellato dal D.Lgs. n. 181/2018) dispone che "*1) Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. 2) Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta*".
Pertanto, ogni Designato di Unità Dirigenziale e chi ha la rappresentanza e il coordinamento degli Organismi è individuato quale "**designato/delegato al trattamento dei dati**", con compiti di riferimento relativamente ai servizi e uffici di competenza.

Il Delegato è designato dal Titolare con apposito atto formale, accompagnato da puntuali indicazioni operative per il corretto assolvimento dei compiti in materia di protezione dei dati, da notificarsi per iscritto al Delegato.

Il Delegato al trattamento dei dati personali, relativamente al proprio settore di competenza, risponde al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di riservatezza, sicurezza, protezione dei dati; riferisce periodicamente al Titolare in ordine alle modalità di svolgimento dei compiti assegnati; verifica che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, rispondano ai principi di necessità, minimizzazione, pertinenza e non eccedenza, segnalando al Titolare eventuali situazioni di potenziale rischio.

Deve rispettare e uniformare la propria attività alle seguenti specifiche prescrizioni indicate nell'atto di designazione a "DESIGNATO E DELEGATO AL TRATTAMENTO DEI DATI PERSONALI".
Il Delegato al trattamento dei dati è dotato di autonomia gestionale ed organizzativa per il trattamento dei dati di propria competenza ed è tenuto ad adottare ogni misura necessaria per il rispetto della riservatezza nell'erogazione delle prestazioni e dei servizi in favore del titolare del dato.

3.3 Soggetto autorizzato del trattamento (ex Incaricato)

CRC designa come "Soggetto autorizzato del trattamento" tutto il proprio personale; contestualmente all'assunzione, l'ufficio Risorse Umane fornisce l'informativa e la lettera di nomina a "Soggetto autorizzato del trattamento".

CRC può designare come soggetti autorizzati (Incaricati) anche persone fisiche (esterne a CRC) che, per esigenze legate alle attività contrattualizzate, partecipano ai trattamenti di dati personali di cui CRC è Titolare.

Ogni soggetto autorizzato deve attenersi alle istruzioni ricevute dal titolare o dal Designato.

3.4 Amministratori di sistema

CRC adotta le misure di sicurezza necessarie ad adempiere alle prescrizioni definite dal Garante nel Provvedimento[1] dedicato alla figura dell'Amministratore di Sistema.

CRC ha definito specifiche procedure operative per disciplinare i seguenti aspetti:

- selezione e nomina degli Amministratori di Sistema (sia per il personale interno che per i consulenti), attribuzione privilegi, aggiornamento dell'elenco degli amministratori di sistema e relativa formazione obbligatoria
- modifica e revoca delle nomine degli Amministratori di Sistema e dei relativi privilegi prevedendo il successivo aggiornamento del suddetto elenco
- verifica dell'attività degli Amministratori di Sistema

[1] Provvedimento Garante del 27 novembre 2008 - Gazzetta Ufficiale n. 300 del 24 dicembre 2008 (modificato in base al provvedimento del 25 giugno 2009), "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

- gestione dei contratti di outsourcing e introduzione in questi ultimi delle opportune clausole per gli adempimenti Privacy in materia di Amministratori di Sistema
- gestione delle richieste da parte degli interessati di consultazione dell'elenco degli Amministratori di Sistema.

Nell'ambito di CRC, il Responsabile Protezione Dati o un soggetto dallo stesso delegato provvede alla verifica almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

3.5 Responsabile della protezione dati (Data Protection Officer)

Il Titolare del trattamento ha designato il **Responsabile della protezione dei dati** / **Data Protection Officer** (in seguito indicato con "RPD" o "DPO").

Il Responsabile Protezione Dati - RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare, ai Designati interni e al Responsabile esterno del trattamento coinvolto nelle attività di trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o ai Designati interni i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile esterno del trattamento.
Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile esterno del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile esterno del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare al Garante;

f) altri compiti e funzioni a condizione che il Titolare del trattamento si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi.
L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

Il Titolare del trattamento assicura che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Designati di specifiche funzioni interne che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

4. Riservatezza dei dati e delle informazioni

Il Personale deve sempre usare la massima discrezione sui dati personali e procedure in corso di cui sia a conoscenza, curando attentamente la loro protezione.

Per assicurare tale discrezione è importante che gli spazi operativi destinati al ricevimento degli utenti o cittadini, alla raccolta dei documenti ed alla loro conservazione siano opportunamente delimitati, per evitare il fortuito accesso da parte di terzi o di personale non interessato. Anche le comunicazioni tra colleghi di dati personali di terzi deve limitarsi a quanto necessario per l'espletamento del servizio.

E' vietata ogni comunicazione di dati all'esterno di CRC, salvo il caso in cui ciò sia necessario per lo svolgimento degli incarichi affidati.

Ogni informazione, sia che si tratti di attività attuali sia che si tratti di attività future, ed ogni altro materiale utilizzato o prodotto dai prestatori d'opera (dipendenti, consulenti o incaricati di ditte esterne) in relazione al proprio impiego/attività, è di proprietà di CRC.

E' vietato copiare, diffondere, pubblicare, inviare notizie e/o informazioni tecniche che in qualche modo possano ridurre la sicurezza di funzionamento d'impianti o reti o che in qualche modo possano permettere di arrecare danni, anche di immagine, alla struttura di CRC.

E' opportuno che ogni dipendente o collaboratore di CRC, salvo espressa autorizzazione o in ragione del ruolo ricoperto, qualora dovesse rilasciare comunicazioni o interviste a nome e per conto della stessa deve comunicarlo preventivamente ai propri responsabili.

5. Trattamenti dei dati personali

Tutti i settori e uffici di CRC sono responsabili di verificare, prima dell'effettivo trattamento, la necessità di operare su dati personali; nel caso si presenti tale fattispecie e se si tratta di categorie particolari di dati o dati giudiziari, le stesse funzioni coinvolgono il Responsabile Protezione dei Dati per concordare con questo le modalità di trattamento.

In particolare, i casi che richiedono specifici presidi sono quelli relativi a:

- trattamenti di dati biometrici;
- trattamenti di dati sensibili e giudiziari;
- trattamenti di dati di minori;
- trattamenti di dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo ("profilazione");
- trattamenti di dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- trasferimento di dati personali verso Paesi extra Ue.

In dettaglio, tutte le funzioni che in CRC raccolgono, utilizzano e conservano i dati personali devono:

- mantenere i dati personali in modo accurato e aggiornato per tutto il ciclo di vita degli stessi (dalla raccolta alla distruzione);
- garantire la sicurezza dei dati personali, nel rispetto delle Policy e delle Procedure di CRC in materia di sicurezza delle informazioni;
- impedire l'utilizzo improprio dei dati personali per uno scopo che non è compatibile con lo scopo originale per il quale i dati sono stati raccolti;
- conservare i dati personali solo per la durata necessaria allo scopo indicato nell'informativa o per il tempo previsto dalla legge.

5.1 Archiviazione

CRC e il personale dipendente devono garantire che i dati personali siano archiviati e trattati in modo sicuro, con misure appropriate alla loro riservatezza e sensibilità. Deve essere prestata particolare attenzione alla memorizzazione dei dati personali su supporti rimovibili, dispositivi portatili o sistemi di storage di terze parti (ad es. cloud storage).

5.2 Trasferimento

Se i dati personali sono trasferiti elettronicamente o manualmente all'interno dell'organizzazione o verso soggetti esterni, deve essere garantita la riservatezza delle informazioni trattate (ad esempio, per i trasferimenti elettronici, utilizzando la crittografia).

5.3 Controllo accessi

CRC deve garantire che, laddove sia consentito l'accesso ai dati personali da parte dei propri dipendenti e collaboratori, tale accesso deve essere autorizzato e limitato al solo personale per il quale è previsto il trattamento nell'ambito dello svolgimento delle proprie mansioni lavorative.

CRC deve informare il personale che l'accesso ai dati personali è valido solo a scopo lavorativo e per scopi legittimi.

Se vengono trattati dati personali ad alto rischio, CRC deve garantire che i meccanismi di controllo accessi implementati siano adeguati a proteggere la sensibilità di queste informazioni.

CRC deve monitorare gli accessi ai dati personali e tenere conto di eventuali violazioni nell'ambito della valutazione del rischio per la sicurezza delle informazioni.

6. Sicurezza del trattamento[2]

Il Titolare del trattamento mette in atto, con l'ausilio degli Amministratori del sistema informatico interni o di società esterne di servizi IT a cui viene delegata l'attuazione, misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio/Unità Dirigenziale/Organismo cui è preposto ciascun Delegato:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro), back up e procedure di disaster recovery/business continuity;
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

Il Titolare e ciascun Designato preposto a Unità Dirigenziale o rappresentante di un Organismo si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6.1 Minimizzare il trattamento dei dati personali rispetto alle finalità individuate

CRC deve mettere in atto misure tecniche e organizzative per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento, sia per quanto riguarda la quantità dei dati personali raccolti che per il periodo di conservazione.

Tali misure devono garantire che, per impostazione predefinita, i dati personali trattati non siano resi accessibili a un numero indefinito di persone senza l'autorizzazione dell'interessato.

In fase di definizione di un nuovo processo, o di progettazione di un nuovo sistema informativo utilizzato per il trattamento dei dati personali, deve essere garantito che:

---

[2] NdR: l'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

- il trattamento sia ridotto al minimo per impostazione predefinita;
- vengano utilizzati, ove possibile, dati non riconducibili direttamente alle persone fisiche;
- le funzionalità implementate siano trasparenti rispetto al trattamento dei dati personali.
- venga conservata adeguata documentazione sulle attività di "privacy by design" implementate e sui risultati ottenuti.

Per ciascun trattamento, deve essere definito il periodo di conservazione dei dati personali, individuando alternativamente:

- l'eventuale periodo minimo di conservazione richiesto dai termini di legge, oppure il periodo minimo di conservazione stabilito da policy interne di CRC;
- una giustificazione documentata dei criteri che determinano il periodo di conservazione.

Al termine del periodo di conservazione stabilito, tutte le copie dei dati personali non più richiesti per le attività operative di CRC devono essere rimossi, facendo riferimento alle procedure di cancellazione (o anonimizzazione) definite da CRC (per il tramite della funzione IT).

Qualora i dati personali debbano essere trasferiti per la conservazione a lungo termine (ad esempio per dati che hanno un valore ai fini dell'archiviazione nell'interesse pubblico), devono essere sottoposti a misure tecniche e organizzative appropriate in modo da salvaguardare i diritti e le libertà dell'interessato.

7. Registro delle attività di trattamento

Il Registro è tenuto in forma telematica/cartacea dal DPO ovvero da un soggetto delegato dal Titolare, presso gli uffici della struttura organizzativa a cui appartengono detti soggetti.

Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

a) il nome ed i dati di contatto di CRC, degli eventuali Contitolari del trattamento e del RPD;
b) le finalità del trattamento;
c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

8. Valutazioni d'impatto sulla protezione dei dati (DPIA)

Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una **valutazione dell'impatto** del medesimo trattamento (**DPIA**) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;
b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 e 10 del RGDP;
e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei

dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

Il Titolare, al fine di individuare un obbligo di DPIA, attua i provvedimenti di settore emanati dall'Autorità Garante per la protezione dei dati personali, da ultimo l'"Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018 (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018) - Registro dei provvedimenti n. 467 dell'11 ottobre 2018.

9. Violazione dei dati personali (Data Breach)

Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati da CRC.

Possiamo considerare realizzata una violazione di dati nei seguenti casi:

- Lettura (presumibilmente i dati non sono stati copiati);
- Copia (i dati sono ancora presenti sui sistemi del titolare);
- Alterazione (i dati sono presenti sui sistemi ma sono stati alterati);
- Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione);
- Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione).

Il personale addetto al trattamento qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti di sicurezza che possano esporre a rischio di violazione dei dati (data breach) deve tempestivamente informare il Titolare, attraverso il Responsabile della Protezione dei Dati.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. *La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo*, utilizzando la procedura operativa predisposta (DPMS 04-001 - Gestione Data Breach).

Anche l'eventuale Responsabile esterno del trattamento nominato è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione entro 24 ore. E' opportuno, pertanto, che ciascun contratto di servizi preveda clausole specifiche al riguardo.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;

- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari,
- giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.

10. Riscontro delle richieste di accesso ai dati personali

Ogni Designato responsabile di settore/direzione o rappresentante di un Organismo, in collaborazione con il Responsabile Protezione Dati, ha la responsabilità di gestire le richieste da parte degli interessati pervenute a CRC relativamente alle casistiche identificate dagli artt. 15-22 e seguenti del Regolamento UE 2016/679, utilizzando la procedura operativa predisposta (vd. Mod. DPMS 03-001).

Il Designato di Unità Dirigenziale o rappresentante di un Organismo, in collaborazione con il Responsabile della Protezione dei Dati, deve assicurare che l'interessato riceva riscontro alla sua richiesta entro 30 giorni. A tal fine il Designato di Unità Dirigenziale o rappresentante di un Organismo è supportato:

- dall'ufficio competente;
- dagli esperti legali per definire il testo della risposta;
- dalla funzione IT interna;
- dagli outsourcer per raccogliere i dati personali, eventualmente trattati dai sistemi informatici, necessari a fornire il riscontro richiesto.

11. Comunicazione e diffusione dei dati

Una specifica attenzione va dedicata alle ipotesi di comunicazione o diffusione dei dati. In altri termini, ogni qual volta si prospetti l'eventualità di divulgare (in qualsiasi forma o modo) dati personali, è necessario procedere alle seguenti verifiche, specie se a riguardo di dati sensibili:

- verifica della legittimità della divulgazione alla luce della informativa fornita all'interessato;
- verifica di eventuali normative e regolamenti che consentano/rendano obbligatoria la divulgazione.

11.2 Condividere e comunicare i dati personali

I dati personali possono essere condivisi con altre società, autorità pubbliche, agenzie governative o soggetti terzi (pubblici e/o privati) nel rispetto delle leggi vigenti e del Regolamento UE 2016/679.

In caso di condivisione con soggetti terzi di dati personali di cui CRC è titolare, si deve ottenere la garanzia che il soggetto terzo abbia la capacità e l'intenzione di proteggere tali dati in conformità agli standard e ai principi espressi dalla presente Policy.

Un contratto per il trattamento dei dati è richiesto ogniqualvolta a un soggetto terzo abbia accesso ai dati personali di cui CRC è titolare per elaborarli per conto della stessa CRC. Tutti i contratti devono comprendere i principi generali e le condizioni per il trattamento dei dati personali.

11.3 Condividere i dati personali con soggetti terzi

CRC deve assicurare che, in caso di condivisione di dati personali con un altro soggetto, le responsabilità di entrambe le parti riguardo la protezione delle informazioni siano formalmente documentate in un accordo o contratto scritto.

Tale contratto deve garantire che, laddove il soggetto terzo utilizzi i dati personali per le proprie finalità:

- siano esplicitamente riportate le finalità per le quali le informazioni possono essere utilizzate dalla terza parte, con eventuali limitazioni o restrizioni sull'ulteriore utilizzo per altri scopi;
- il soggetto terzo fornisca una prova del proprio impegno nei confronti di CRC per garantire il trattamento dei dati personali in modo da non contravvenire alla legislazione vigente.

Ogni nuovo trattamento che comporta la condivisione di dati personali con terze parti deve essere conforme con quanto indicato nell'informativa fornita all'interessato.

CRC deve assicurarsi inoltre di avere:

- una base legale per la condivisione dei dati;
- di aver fornito un'adeguata comunicazione all'interessato della condivisione dei dati;
- di aver tenuto in considerazione il principio di limitazione delle finalità del trattamento;
- di aver ottenuto il consenso dell'interessato, dove previsto.

12. Trasferire i dati personali all'estero (extra UE)

In alcuni casi dati personali possono essere condivisi con soggetti terzi che operano all'estero nel rispetto delle prescrizioni previste dal Regolamento UE 2016/679.

12.1 Trasferire i dati personali al di fuori dell'Unione Europea solo con adeguate garanzie

Qualora si renda necessario il trasferimento dei dati personali al di fuori dell'Unione Europea, CRC deve garantire la protezione dei diritti e delle libertà degli interessati:

- includendo nei contratti con le terze parti condizioni specifiche per assicurare la protezione dei dati personali;
- verificando la conformità rispetto ad un codice di condotta o ad un meccanismo di certificazione del soggetto terzo;
- mettendo in atto regole aziendali vincolanti interne nel caso in cui il trasferimento avvenga verso un'altra entità (es. del Gruppo o una controllata) che si trova al di fuori dell'Unione Europea.

13. Misure di sicurezza per il trattamento di dati personali effettuato senza strumenti elettronici

In particolare, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento effettuate senza l'ausilio di strumenti elettronici, chiunque tratti dati all'interno di CRC deve conservare gli atti, i documenti e ogni altro supporto contenente dati personali in ambienti controllati (ad esempio, locali, armadi o cassetti muniti di serratura), prelevandoli per il solo tempo necessario al loro utilizzo e restituendoli a chi ne ha la responsabilità e l'autorizzazione alla conservazione, al termine delle operazioni affidate. Nel dettaglio:

a) il materiale cartaceo contenente dati personali deve essere controllato e custodito con diligenza in modo da impedire che durante le quotidiane operazioni di lavoro terzi non autorizzati possano prenderne visione e, se il materiale contiene dati sensibili o giudiziari, esso dovrà essere conservato, sino alla restituzione, in contenitori muniti di serratura. Al termine del lavoro tutto il materiale dovrà essere riposto in armadi, cassetti o altri contenitori muniti di serratura, in maniera che ad essi non accedano persone prive di autorizzazione;

b) l'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato;

c) gli atti ed i documenti contenenti categorie particolari dati personali (sensibili) o giudiziari sono affidati al personale esclusivamente per lo svolgimento dei relativi compiti assegnati in forma scritta: i medesimi atti e documenti sono controllati e custoditi dai predetti soggetti fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;

d) il personale ammesso, a qualunque titolo, agli archivi contenenti dati sensibili o giudiziari, dopo l'orario di chiusura, sono identificati e registrati: 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;

e) è obbligatorio distruggere o rendere inutilizzabili i documenti cartacei ed i supporti rimovibili, magnetici o ottici dismessi in modo da garantire che i dati ivi contenuti non possano più essere ricostruiti e/o utilizzati (anche parzialmente) da parte di terzi non autorizzati al trattamento: anche il materiale destinato al macero ed i supporti magnetici o ottici da eliminare devono essere trattati in modo che risulti tecnicamente impossibile recuperare, anche parzialmente, i dati contenuti negli stessi. Pertanto occorre prevederne la distruzione (se disponibili, con le apposite macchine "distruggi documenti/supporti" o con tecnologie similari) in modo da garantire che i dati in essi contenuti non possano essere ricostruiti, anche parzialmente, o utilizzati;

f) tutte le stampe effettuate, contenenti dati personali, dovranno essere trattate in modo da evitare che terzi non autorizzati possano prenderne visione oppure accedervi e/o produrne copie.

Il Designato di Unità Dirigenziale o il rappresentante di un Organismo verifica la corretta applicazione da parte degli autorizzati di tutte le procedure previste in materia di trattamenti effettuati.

Tale designato o rappresentante verifica in particolare che l'accesso agli archivi cartacei sia consentito al solo personale autorizzato e che la distruzione dei supporti cartacei che contengono dati personali venga effettuato in conformità alla normativa vigente.

14. Misure di sicurezza per il trattamento di dati personali effettuato con strumenti elettronici (Regole per l'utilizzo di strumenti informatici)

Il Titolare e il Personale autorizzato al trattamento dei dati, qualora durante lo svolgimento della loro attività lavorativa utilizzino strumenti informatici devono rispettare quanto previsto dal "**REGOLAMENTO PER L'UTILIZZO DEGLI STRUMENTI ELETTRONICI, DI INTERNET E DELLA POSTA ELETTRONICA**" (Vd. Mod. DPMS 02-001).

15. Smaltimento o riuso di apparecchiature elettriche ed elettroniche

Ogni Designato di Unità Dirigenziale o rappresentante di un Organismo è responsabile dell'adozione di opportune misure di sicurezza, anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, per garantire l'inesistenza o la non intelligibilità di dati personali sui supporti di memorizzazione destinati al reimpiego, al riciclaggio o allo smaltimento. In tali casi, è necessario consultare preventivamente i responsabili IT interni.

16. Verifiche periodiche

Oltre alla normale verifica delle attività operative in capo al Designato di Unità Dirigenziale o rappresentante di un Organismo, sono previste verifiche periodiche in accordo con la normativa vigente, al fine di **verificare il rispetto della presente Politica generale per il trattamento dei dati personali.**

CRC si riserva comunque le facoltà previste dalla normativa vigente di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno, che ledono diritti di terzi o che, comunque, risultino illegittime.

All'interno del Modello Organizzativo per la Protezione Dati previsto da CRC (Data Protection Management System, c.d. DPMS), le attività di valutazione delle misure organizzative, procedurali e tecniche sono in carico del Responsabile della Protezione dei Dati o altri professionisti esterni.

Riguardo a tali controlli il presente Regolamento costituisce preventiva e completa informativa nei confronti dei dipendenti e collaboratori.

ATTUAZIONE

Formazione e Consapevolezza

CRC deve garantire che tutti i dipendenti e i collaboratori siano informati sui principi espressi dalla presente Politica e che comprendano le responsabilità derivanti dal trattamento dei dati personali.

CRC deve assicurare che tutto il personale che tratta dati personali prenda parte alla formazione fornita periodicamente in base al proprio ruolo istituzionale.

La documentazione relativa alla partecipazione del personale alla formazione deve essere conservata come evidenza delle competenze acquisite.

Riferire potenziali inadempienze

Qualsiasi dipendente che venga a conoscenza di una possibile violazione della presente Politica e/o del Regolamento UE 2016/679 è tenuto a riferire immediatamente al Responsabile della Protezione dei Dati personali (DPO) ovvero ai Designati di Unità Dirigenziale o al rappresentante di un Organismo.

I dipendenti che riferiscono potenziali inadempienze, che forniscono informazioni o che partecipano in altro modo a qualsiasi inchiesta o indagine interna su possibili inadempienze saranno protetti contro le ritorsioni secondo le normative vigenti.

Responsabilità e Implementazione

Ciascun Designato di Unità Dirigenziale o rappresentante di un Organismo ha il compito di rispettare la

presente Politica nella propria area funzionale di responsabilità, per essere da esempio e fornire linee guida a tutti i dipendenti che ad esso riferiscono.

Tutti i dipendenti sono responsabili del rispetto dei principi e delle regole definite nella presente Policy.

SANZIONI

È fatto obbligo a tutti i Dipendenti e collaboratori di CRC di osservare le disposizioni portate a conoscenza con le presenti Istruzioni Operative. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile con provvedimenti disciplinari e/o risarcitori previsti dalla vigente normativa, nonché con tutte le azioni civili e penali consentite.

AGGIORNAMENTO E REVISIONE

La presente Politica è stata redatta tenendo conto della normativa vigente e dei Provvedimenti generali emanati dal Garante della Privacy. Per qualsiasi eventuale ulteriore indicazione, valgono oltre alla presente Politica le disposizioni della normativa vigente.

Tutti i dipendenti e collaboratori possono proporre, quando ritenuto necessario, integrazioni al presente documento. Le proposte vanno esaminate dal Titolare tramite il Responsabile della Protezione dei Dati.

La presente Politica è soggetta a revisione con frequenza periodica o qualora se ne ravveda la necessità.

Copia del presente documento verrà consegnata a ciascun dipendente o collaboratore ovvero messo a disposizione per ogni soggetto autorizzato all'utilizzo della rete aziendale interna.

Con l'entrata in vigore del presente Politica, tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi sostituite dalle presenti.

RINVIO

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.

_____

Allegato 1: GLOSSARIO E PRINCIPALI DEFINIZIONI

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	GDPR
Autenticazione informatica	L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità	
Autorità di controllo	l'Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 e, per l'Italia, il Garante per la protezione dei dati personali	GDPR
Autorità di controllo interessata	un'Autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile [esterno] 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	GDPR
Banca di dati	Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti	
Chiamata	La connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale	
Comunicazione	Il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione	
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile	
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	GDPR
Credenziali di autenticazione	I dati e i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica	
Delegato/Designato	Si tratta di ogni Designato di Unità Dirigenziale o rappresentante di un Organismo che è individuato quale "designato/delegato al trattamento dei dati" e con compiti di riferimento relativamente ai servizi e uffici di competenza	
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	GDPR
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	GDPR
Dati relativi al traffico	qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione	
Dati relativi all'ubicazione	ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico	
Dati relativi alla salute	i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute	GDPR

Categorie particolari di dati	i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, i dati genetici, i dati biometrici, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale	GDPR
Dato anonimo	il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile	
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	GDPR
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	GDPR
Diffusione	l dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione	
Evidenza	nell'ambito della ISO 19011 sono definite evidenze dell'audit le registrazioni, dichiarazioni di fatti o altre informazioni, che sono pertinenti ai criteri dell'audit e verificabili. Possono essere qualitative o quantitative	ISO 19011
Gruppo imprenditoriale	un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate	GDPR
Impresa	la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica	GDPR
Interessato	la persona fisica cui si riferiscono i dati personali	
Limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro	GDPR
Norme vincolanti d'impresa	le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile [esterno] 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 [esterno] 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	GDPR
Obiezione pertinente 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 [esterno] 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	GDPR
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	GDPR
Parola chiave	componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica	
Politica (Policy)	descrive, ad alto livello, la posizione di una organizzazione rispetto ad un determinato argomento. La policy, comportando un'assunzione di rischio, deve essere approvata dal top management	
Procedura	una procedura descrive, con il livello di dettaglio adeguato, come un'organizzazione realizza uno specifico obiettivo. E' possibile che un'organizzazione si doti di un impianto documentale con procedure a diverso	

	livello di dettaglio, dalle più generiche alle istruzioni operative. La modalità, il formato, la responsabilità di creazione e gestione, le modalità di revisione devono essere formalmente definite.	
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	GDPR
Profilo di autorizzazione	l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti	
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	GDPR
Rappresentante	la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile [esterno] del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento	GDPR
Responsabile esterno 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	GDPR
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	GDPR
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, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione	GDPR
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 [esterno] del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile [esterno]	GDPR
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 [esterno] del trattamento nell'Unione ove il titolare del trattamento o il responsabile [esterno] 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 [esterno] del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro	GDPR
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	GDPR
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	GDPR

Regolamento Interno

Regolamento per l'utilizzo degli strumenti informatici, posta elettronica e Internet del Consiglio regionale della Campania

Redatto da:	Giuseppe Ferretti
Approvato da:	Giovanna Donadio
Data creazione:	25.05.2020
Distribuzione:	Solo uso interno
Destinatari:	**Tutto il personale dipendente (Dirigenti / Responsabili di Struttura, Designati, Autorizzati) ed eventuali responsabili esterni del trattamento**
Aggiornato il:	25.05.2020

INTRODUZIONE

In un mercato sempre più competitivo, dove i margini temporali d'azione si riducono in modo esponenziale, una delle chiavi dell'efficacia dei processi è rappresentata sicuramente dalle informazioni che tali processi ricevono, producono, processano e trasmettono.
I moderni sistemi informatici, con il loro prezioso carico informativo, si sono trasformati negli anni in uno dei principali asset sul quale costruire il successo del business e dal quale la sua durata nel tempo può dipendere.
La pronta **disponibilità** delle informazioni, la loro **accuratezza** e **integrità**, la loro **riservatezza** rivestono oggi un ruolo centrale nella tutela del patrimonio informativo.
Difendere questi aspetti significa porre delle solide basi per la continuità del business e per preservare l'immagine dell'Ente.

Con il presente documento, pertanto, s'intende uniformare la gestione e l'utilizzo degli strumenti informatici personali/ collettivi in relazione alle attività svolte all'interno dell'Ente. Attraverso l'utilizzo delle risorse informatiche e telematiche dell'Ente, infatti, si deve evitare che comportamenti inconsapevoli possano generare problemi o minacce alla protezione dei dati personali, agli strumenti e a tutti i documenti rilevanti.
Tutte le tecnologie informatiche e telematiche a disposizione, che vengono fornite configurate in modo sicuro, devono essere utilizzate ispirandosi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro.
Le prescrizioni e le indicazioni che seguono si aggiungono ed integrano le altre policy e le specifiche istruzioni già fornite a tutti gli "autorizzati/incaricati al trattamento".
Per qualsiasi dubbio relativo all'applicazione pratica o all'interpretazione della presente Policy, è possibile rivolgersi al Responsabile della Protezione dei Dati o al Referente ICT.

SCOPO E CAMPO DI APPLICAZIONE

Il Garante per la protezione dei dati personali, con Provvedimento del 1.03.2007 pubblicato sulla G.U.R.I. del 10.03.2007, n. 58, avente ad oggetto "Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori", raccomanda l'adozione da parte dei datori di lavoro pubblici e privati, di un disciplinare interno in cui siano indicate le regole per l'uso di Internet, della posta elettronica e della tenuta di file della rete interna nel rispetto della Legge 20.05.1970, n. 300 (Statuto dei lavoratori) e del Decreto Legislativo 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali) e successive modificazioni ed integrazioni.

Con il presente regolamento, sono disciplinate le condizioni di utilizzo delle risorse informatiche e di comunicazione che l'Ente mette a disposizione dei Lavoratori dipendenti/ Utenti ed Operatori per l'esecuzione delle funzioni di competenza.
Sono altresì regolate le modalità con le quali l'Ente può accertare e inibire le condotte illecite degli utilizzatori di Internet, della posta elettronica e dell'accesso alle risorse di archiviazione di massa (server, hard disk, cloud).

Sono tenuti all'osservanza delle presenti disposizioni tutti gli Utenti Interni ed Esterni che sono autorizzati ad accedere al Sistema Informatico.
Per Utenti Interni si intendono le persone fisiche che, sulla base di rapporti contrattuali o convenzionali autorizzati dal Consiglio e dalle varie Direzioni/ Unità Dirigenziali/ Organismi, possono utilizzare all'interno del "dominio" gli strumenti informatici dell'Ente.
Per Utenti Esterni si intendono: le persone fisiche, le Aziende private e Pubbliche e le ditte fornitrici che, sulla base di rapporti contrattuali o convenzionali autorizzati, accedono dall'esterno del "dominio" ad alcune componenti del Sistema Informatico.
Tali soggetti possono essere individuati come "Designati di specifici compiti e funzioni" o quali "Autorizzati al trattamento" dei dati personali ai sensi del Regolamento UE 2016/679, mentre i soggetti "esterni" all'Ente, nei casi relativi a collaborazione di persone fisiche o giuridiche (convenzioni, consulenze, tirocini, appalti, ecc.), possono operare in qualità di responsabili del trattamento; d'ora in avanti sono denominati tutti anche con il termine "Personale".

All'interno del documento non sempre vengono fornite indicazioni puntuali in quanto, dato l'ambito in

continuo sviluppo, risulterebbe difficile se non impossibile contemplare ogni tipologia di dispositivo informatico e di informazione di interesse. Risulta per tale ragione un fattore chiave comprendere le idee alla base e le finalità del presente documento per poter seguire in modo efficace le indicazioni fornite.
Quanto segue è redatto nel pieno rispetto delle leggi regolatrici dei rapporti di lavoro e del Provvedimento a carattere generale emesso Garante per la protezione dei dati personali il 1° marzo 2007 (relativo all'utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro) ed è pertanto indispensabile la sua conoscenza da parte di tutti i dipendenti e collaboratori dell'Ente.

Una corretta esecuzione del presente Regolamento presuppone il pieno assolvimento da parte dell'Ente degli obblighi contenuti nella Circolare dell'Agenzia per l'Italia Digitale – AGID n. 2 del 18 aprile 2017 relativa alle «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)» e s.m.i., nonché di eventuali provvedimenti in materia emanati da organismi operanti nel medesimo settore.

RIFERIMENTI NORMATIVI E DOCUMENTALI

NORMATIVA EUROPEA

- **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE ("Regolamento Generale sulla Protezione dei Dati personali").

NORMATIVA ITALIANA

- **Decreto Legislativo 30 giugno 2003, n. 196 e successive integrazioni e modificazioni** ("Codice in materia di protezione dei dati personali").

- **Legge 20 maggio 1970, n. 300**, norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento (detta anche "statuto dei lavoratori").

- **Codice Civile**
  - Art. 2049 Responsabilità indiretta dell'imprenditore;
  - Art. 2086 Direzione e gerarchia nell'impresa;
  - Art. 2087 Tutela dell'integrità fisica e della personalità morale dei dipendenti, da parte dell'imprenditore;
  - Art. 2104 Diligenza del dipendente nel rispetto delle disposizioni impartite dall'imprenditore.

PROVVEDIMENTI AUTORITA' GARANTE PRIVACY

- **Linee Guida del Garante Privacy su Posta Elettronica e Internet** (Deliberazione n. 13 del 1 marzo 2007 – G.U. n. 58 del 10 marzo 2007);

- **Provvedimento del Garante Privacy del 27 novembre 2008** e successive modificazioni relativo a "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di sistema";

AGENZIA PER L'ITALIA DIGITALE - AGID

- **Circolare** dell'Agenzia per l'Italia Digitale – AGID n. 2 del 18 aprile 2017 relativo a «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)».

PREMESSE

1) Ai sensi del Regolamento UE 679/2016, i dati possono essere classificati come segue:

- Personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile; 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. Sono dati personali: nome e cognome, indirizzo, codice fiscale, foto, l'indirizzo IP o qualsiasi altra ripresa audiovisiva. La persona difatti può essere identificata anche attraverso altre notizie che non siano direttamente identificative (ad esempio, associando la registrazione della voce di una persona alla sua immagine, oppure alle circostanze in cui la registrazione è stata effettuata: luogo, ora, situazione).

- Categorie particolari di dati: dati personali che, per la propria delicatezza, richiedono particolari cautele; essi sono quei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, nonché i dati relativi alla salute o o all'orientamento sessuale della persona.

- Dati relativi a condanne penali e reati: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (quali dati personali idonei a rilevare provvedimenti emessi dalle Autorità Giudiziarie e contenuti nel casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 c.p.p.)

2) Per **trattamento dei dati** si intende "qualunque operazione o complesso di operazioni concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati". In tale ottica è indifferente che le operazioni vengano svolte con o senza l'ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo sono assoggettati alla normativa privacy.

Pertanto, le operazioni di trattamento si possono idealmente suddividere in tre macro-tipologie, in funzione del fatto che il loro fine sia:

***a) Il reperimento delle informazioni*.**
Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi o un sito web.

***b) Il trattamento "interno" delle informazioni*.**
Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili. Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, eccetera;
- l'elaborazione, ovvero le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;
- la selezione, l'estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni;
- l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;

- la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

c) L'uso delle informazioni nei rapporti con l'esterno.

Sono i trattamenti più delicati, in quanto è con essi che si può concretamente ledere la sfera della riservatezza altrui: essi vengono genericamente definiti come utilizzo, ovvero la realizzazione dello scopo per cui si è provveduto alla raccolta ed ai trattamenti interni.
L'utilizzo può essere:

- diretto, instaurando cioè un rapporto con la persona sul conto della quale si sono raccolte informazioni;
- indiretto, ovvero consistere nel mettere a disposizione di terzi le informazioni raccolte.

Le operazioni di utilizzo cui la legge dedica le maggiori attenzioni, in quanto si tratta di quelle potenzialmente più lesive della privacy, sono quelle con cui si mettono a disposizione di terzi i dati personali. Esse sono:

- la **comunicazione**, cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- la **diffusione**, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

3) Per lo svolgimento delle quotidiane attività lavorative, il Titolare necessita dell'utilizzo di apparecchiature informatiche per l'espletamento di molteplici compiti, nell'ambito di diversi ruoli e posizioni organizzative.
L'uso di tali apparecchiature deve essere disciplinato da norme certe in quanto da comportamenti - anche inconsapevolmente non leciti - possono derivare conseguenze gravi, sia sul piano tecnico (come un blocco della funzionalità o una perdita di dati), sia sul piano giuridico (che possono determinare l'insorgere di responsabilità sia penali sia civili a carico, contestualmente, del Titolare e del lavoratore coinvolto).

4) L'**allegato A)** costituisce parte integrante del presente Regolamento.

NORME COMPORTAMENTALI

1. Norme tecniche

- Tutto il Personale che utilizza strumenti elettronici è tenuto a prendere visione e attenersi a quanto previsto nel presente Regolamento Interno. Tali documenti sono reperibili presso il portale Intranet, sezione "Privacy".

- Il Personale che tratta dati personali è tenuto al rispetto di tutte le apparecchiature messe a disposizione dall'Ente, provvedendo alla buona conservazione delle stesse, avendo cura al termine dell'orario di lavoro di lasciare la propria postazione di lavoro ordinata, efficiente e **con le apparecchiature spente** (se non diversamente previsto da elaborazioni che proseguono oltre l'orario di lavoro). Al momento di lasciare i locali e gli uffici, il personale dovrà altresì accertarsi della chiusura di finestre dei locali da loro occupati.

- I personal computer ed i dispositivi mobili utilizzati dagli Utenti Interni sono strumenti di lavoro. Ogni utilizzo improprio può causare disservizi, costi impropri di manutenzione e, soprattutto, minacce alla sicurezza ed alla privacy. Nei PC forniti è sconsigliato l'inserimento di supporti magnetici o ottici esterni (CD-ROM, DVD–ROM, Pen Drive, etc.), se non espressamente autorizzati o verificati dal Referente ICT.

- Gli Utenti non devono modificare la configurazione del proprio PC; in caso di malfunzionamento dovranno richiedere l'intervento dei tecnici preposti. Si fa inoltre assoluto divieto di installare sulle apparecchiature software non autorizzati. Si ricorda che il mancato rispetto delle norme relative alle licenze d'uso è perseguibile penalmente.

- E' assolutamente vietato modificare i dati contenuti nei programmi gestionali, salvo quelli esplicitamente autorizzati ed è altresì vietato effettuare modifiche, attraverso gli strumenti di sviluppo, di qualsivoglia componente dei programmi stessi.

- Tutta la documentazione prodotta dal personale autorizzato al trattamento dovrà essere elaborata con gli strumenti messi a disposizione dall'Ente e dovrà essere inserita nelle cartelle autorizzate (anche eventualmente in cloud); periodicamente verrà effettuato un controllo dei dischi fissi al fine di verificarne l'efficienza, provvedendo all'eliminazione dei file superflui. È fatto divieto di salvare file e/o cartelle in posizioni non autorizzate.

- Non è consentita la memorizzazione, su qualsiasi supporto, di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

- Poiché i malware, ovvero un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al sistema su cui viene eseguito (rientrano in questa categoria: virus, worm, spyware e altri programmi dannosi), costituiscono una delle minacce più frequenti alla sicurezza, è necessario che il Personale incaricato al trattamento si attenga alle seguenti norme:
  - il sistema informatico presenta software di protezione che vengono aggiornati automaticamente; si raccomanda, pertanto, di verificare periodicamente l'effettivo funzionamento del sistema e di non disattivarli in nessuna occasione;
  - è necessario evitare di scaricare / caricare materiale che potrebbe contenere virus o altri software dannosi;
  - non scaricare mai file da mittenti sconosciuti o sospetti e, quando necessario, effettuare sempre un controllo prima di acquisire o aprire qualunque programma o documento acquisito via posta elettronica (in caso di dubbio contattare i tecnici informatici dell'help desk del CRC).

2. Sistemi informativi

- Salva schermo protetto con password
  All'interno della rete i dispositivi sono protetti da una impostazione del sistema operativo che, dopo un breve periodo di inattività dell'elaboratore, lo blocca attivando uno screen-saver protetto con password. Ciononostante, il Personale è tenuto a bloccare il proprio computer (fisso o laptop) nella pause previste o nel momento in cui debba allontanarsi da esso per più di qualche minuto.

- Unità Disco di rete / Cloud
  L'Ente dispone dei così detti "Dischi di Rete". Si tratta di spazi di memorizzazione dedicati ai file degli utenti e che vengono protetti con sistemi avanzati di backup. Questa protezione garantisce la disponibilità del dato in caso di perdita o danneggiamento dei dispositivi locali di memorizzazione. I file che vengono prodotti in locale devono essere salvati anche nel disco di rete e, una volta che non sussistano più ragioni di convenienza, i file locali devono essere eliminati a favore della sola conservazione sul disco di rete.
  Le cartelle nei dischi di rete possono essere create per area e per un singolo dipendente. Vedere anche il punto successivo per la cartella personale nei dischi di rete.

- Cartella personale
  Nei dischi di rete è presente una cartella (dedicata o nominativa) per il salvataggio dei propri dati. In tale cartella devono essere salvati tutti i file del personale dipendente, anche se memorizzati inizialmente in locale su personal computer e laptop.
  In caso di furto o smarrimento dei dispositivi portatili, infatti, la copia "in rete" dei file garantirà la disponibilità delle informazioni. Come già evidenziato in precedenza si invitano tutti i dipendenti a mantenere le sole informazioni necessarie sul disco locale, utilizzando principalmente il disco di rete al fine di garantirne la disponibilità e la riservatezza in caso di eventi dannosi.

- Cartelle locali

Le cartelle create localmente nei personal computer e laptop sono da intendersi come temporanee e l'eventuale contenuto deve esistere in copia di sicurezza anche nei dischi di rete.
Il loro uso tipico è quello di permettere al personale dipendente di lavorare su file anche quando si trova al di fuori della rete interna.

- Supporti di memorizzazione
  Occorre salvare sempre le informazioni confidenziali sul server di rete e non all'interno della postazione locale, non salvare informazioni di natura sensibile su supporti rimovibili e, nel caso in cui le pen drive siano consegnate a terzi per trasferire dati, assicurarsi che sulla pen drive siano presenti solamente i dati necessari da trasferire, ovvero effettuare personalmente l'operazione di trasferimento, evitando di consegnare la pen drive a terzi, che potrebbero duplicare per scopi illeciti le informazioni personali ivi memorizzate.
  Eliminare sempre documenti, dischi, pen drive o altri supporti di memorizzazione in maniera sicura, evitando di gettarli nel cestino della spazzatura, senza averli previamente resi inutilizzabili e accertarsi che le informazioni non più utili vengano cancellate in modo sicuro dai supporti di dati e non conservare inutilmente messaggi di posta elettronica.

- Utilizzo di dispositivi mobili (notebook, tablet)
  In caso di necessità, i dispositivi mobili del CRC vengono assegnati individualmente a singoli utenti interni, che rispondono del loro utilizzo e devono custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo intra ed extra lavorativo.
  Occorre prestare attenzione a non lasciare mai incustodito tale strumento in ufficio o in viaggio (particolare attenzione deve essere riposta quando si viaggia sui mezzi pubblici).
  Durante le missioni di lavoro, portare il dispositivo mobile come bagaglio a mano, evitando di trasportare nella medesima borsa i codici identificativi e le parole chiave di sicurezza, nonché i supporti di memorizzazione con le copie di back-up.
  Non lasciare esposto in automobile in sosta il dispositivo mobile assegnato.

- Software
  Sugli strumenti in dotazione può essere utilizzato solamente il software fornito dall'Ente; pertanto, non si possono acquistare e installare altri software e applicazioni senza una specifica verifica e autorizzazione da parte della UD Sistemi Informativi del CRC.
  Non installare da soli i software sul personal computer in dotazione, se non previa autorizzazione, e non creare e non utilizzare software senza licenza d'uso (D.lg. 518/92 sulla tutela giuridica del software e L. 248/2000 sulle nuove norme di tutela del diritto d'autore).

3. Accesso ed uso dei sistemi e password

- Le unità disco (locali o di rete o in cloud) sono aree di condivisione di informazioni strettamente lavorative e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia connesso all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. È vietata, anche, la conservazione e l'archiviazione dei dati in disco locale sui singoli PC, salvo alcune specifiche eccezioni legate a esigenze produttive.

- Il personale dipendente si connette alla rete dell'Ente tramite autenticazione univoca personale (credenziali account + password). Il titolare della password è tenuto a non rivelarla ad alcuno, (colleghi, superiori amministratori di sistema inclusi), dovendo avere la massima diligenza nella custodia della stessa e preservandone la segretezza anche durante il momento della digitazione. Qualora il dipendente prenda coscienza che taluno possa aver visionato la digitazione o essere comunque a conoscenza della password, deve immediatamente cambiarla. Qualora sia richiesto di riferire in qualunque forma la password (telefonicamente, via e-mail, etc.) il personale è obbligato a rifiutarsi; contemporaneamente deve dare immediata comunicazione dell'accaduto alla UD Sistemi Informativi del CRC.

- Non debbono essere utilizzate, nella configurazione delle caselle di posta elettronica, le opzioni di "compilazione automatica" o "remember password", presenti nei browser o in altre applicazioni.

- È vietato comunicare, scambiare o condividere password tra più utenti (neanche se appartenenti al medesimo team di lavoro) o divulgare password personali a terzi (anche se colleghi o amministratori di sistema); la condotta non conforme a questa prescrizione può comportare sanzioni disciplinari.

- La password scelta non deve avere relazione con la propria vita privata e deve essere scelta secondo i requisiti minimi di complessità comunicati ed aggiornati dalla UD Sistemi Informativi del CRC.

- È vietato riutilizzare le proprie password lavorative (es. di accesso al PC, alla posta o ai vari applicativi) per la registrazione in altri siti web.

- Il Personale ha l'obbligo di cambiare la password di accesso agli strumenti informatici almeno ogni 90 giorni. Solo in casi eccezionali la password potrà essere resettata a cura dei tecnici della UD Sistemi Informativi del CRC.

- Occorre conservare le password con diligenza, per impedire che soggetti terzi ne vengano a conoscenza, segnalandone sollecitamente al personale della UD Sistemi Informativi del CRC l'eventuale smarrimento, sottrazione o diffusione.

- In nessun caso devono essere annotate password in chiaro, sia su supporto cartaceo sia informatico. I requisiti minimi di complessità delle password sono:
  - redazione con caratteri maiuscoli e/o minuscoli;
  - utilizzo di simboli, numeri, punteggiatura e lettere;
  - la lunghezza della password deve essere di almeno 8 caratteri;
  - non deve trattarsi di password basate su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente al soggetto titolare della password stessa.

  La password deve essere mantenuta segreta, adottando gli opportuni accorgimenti per la sua custodia.

4. Posta Elettronica

- Il servizio di Posta elettronica viene fornito, dall'Ente, in funzione della comunicazione, della amministrazione e delle altre attività strumentali correlate ai fini istituzionali. Il servizio è subordinato all'osservanza integrale delle condizioni contenute nel presente documento. L'utilizzo del servizio da parte dell'Utente costituisce implicita accettazione delle citate condizioni.

- Sono attivati indirizzi di posta elettronica per le strutture interne (Organi consiliari, Commissioni, Direzioni Generali, Unità Dirigenziali, etc.), condivisi dagli operatori assegnati a ciascuna di esse, con il nome a dominio **@cr.campania.it**.
  Al singolo Lavoratore dipendente/ Utente può essere assegnato un indirizzo e-mail personale del tipo: **cognome.prime3letterenome@cr.campania.it** con eccezioni previste per i casi di omonimia.

- La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà dell'Ente, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative; non è consentito l'utilizzo per motivi diversi da quelli inerenti all'espletamento degli adempimenti lavorativi.

- L'Utente si impegna ad adoperarsi attivamente per salvaguardare la riservatezza della propria password e a segnalare qualunque situazione che possa inficiarla. L'Utente sarà responsabile dell'attività espletata tramite il proprio account.

- Il Personale dipendente o l'Utente, salvo giustificabili eccezioni, di cui comunque risponde personalmente, non può utilizzare la posta elettronica per inviare, anche tramite collegamenti o allegati in qualsiasi formato (testo, fotografico, video, grafico, audio, codice, ecc.), messaggi che contengano o rimandino a: i) comunicazioni commerciali private; ii) materiale in violazione della Legge n. 269 del 1998; iii) materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.; iv) materiale che violi le normative sulla privacy; v) contenuti o materiali che violino i diritti di proprietà di terzi; vi) altri contenuti illegali. L'elenco riportato è da intendersi meramente indicativo e non esaustivo. In nessun caso l'Utente potrà utilizzare la posta elettronica istituzionale per diffondere codici dannosi per i computer quali virus e simili.

- Si deve evitare di rispondere alle "catene di Sant'Antonio" degli utenti di internet o ai messaggi di solidarietà che richiedono di inviare un'e-mail a un certo indirizzo o a un certo numero di utenti, poiché possono essere veicoli di diffusione di virus informatici ovvero sistemi per la raccolta di

indirizzi di posta elettronica, per l'invio di comunicazioni commerciali non desiderate o di posta "spazzatura", nonché si deve evitare di rispondere a messaggi promozionali o di spamming.

- È fatto divieto di accedere, in modo non autorizzato, ad altri account, a sistemi o ad altre reti tramite operazioni di pirateria informatica, contraffazione della password o altri mezzi illeciti o fraudolenti.

- Si rende noto che per motivi organizzativi e funzionali, vengono archiviati tutti i messaggi di posta elettronica (anche nelle copie di back up), in uscita ed in entrata dalle caselle di posta elettronica dell'Ente. Conseguentemente, stante la natura di strumento di comunicazione istituzionale del sistema di posta elettronica, il personale dipendente è consapevole che sullo stesso non potrà essere garantita la riservatezza dei del messaggio e dei documenti inviati e ricevuti; pertanto, sarà impegno del personale dipendente evitare l'utilizzo delle caselle di posta elettronica per comunicazioni di carattere personale o che esulino dal contesto Entele a cui sono preposte.

- Nei messaggi inviati tramite posta elettronica istituzionale (di servizio e/o nominative) verrà accluso il seguente testo: "*Si segnala che il presente messaggio e le risposte allo stesso potranno essere conosciute dall'organizzazione lavorativa di appartenenza del mittente secondo le modalità previste dal regolamento adottato in materia. Se per un disguido avete ricevuto questa e-mail senza esserne i destinatari vogliate cortesemente distruggerla e darne informazione all'indirizzo mittente*".

4.1 Posta Elettronica Certificata (PEC)

- La Posta Elettronica Certificata (detta anche PEC) è un sistema di comunicazione simile alla posta elettronica standard ma tra indirizzi mail certificati, a cui si aggiungono caratteristiche di sicurezza e di certificazione della trasmissione tali da aggiungere valore legale ai messaggi trasmessi.
  Il **valore legale** è assicurato dai gestori di posta PEC del mittente e del destinatario che certificano:
  - data e ora dell'invio del messaggio dal parte del mittente;
  - data e ora dell'avvenuta consegna del messaggio al destinatario;
  - integrità del messaggio (e eventuali allegati) nella trasmissione da mittente a destinatario.
  I gestori di posta assicurano anche notifica al mittente e al destinatario di eventuali problemi occorsi durante la trasmissione.

- La PEC trasferisce sul digitale il concetto di "**Raccomandata con Ricevuta di Ritorno**". L'utilizzo della posta elettronica rispetto alla posta tradizionale garantisce la consegna in tempo reale.
  Valore legale: a differenza della tradizionale posta elettronica, alla PEC è riconosciuto pieno valore legale e le ricevute possono essere usate come prove dell'invio, della ricezione ed anche del contenuto del messaggio inviato.
  La comunicazione ha valore legale solo se inviata da PEC e ricevuta su PEC.

  Le caselle PEC del CRC hanno estensione: **@pec.cr.campania.it.**
  Esse accettano normalmente messaggi e documenti provenienti sia da caselle di PEC che non PEC, al fine di garantire possibilità di comunicazione anche agli utenti non dotati di PEC (ad es. per la corrispondenza indirizzata a Garanti, Difensore Civico, etc.).
  Gli indirizzi PEC istituzionali che possono essere utilizzati per le finalità come sopra rappresentate sono elencati nell'Indice IPA:
  https://www.indicepa.gov.it/ricerca-pec/n-ricerca-pec.php?cod_amm=cr_campa&mail_pec=

4.2 Liste di distribuzione

- Allo scopo di facilitare l'interscambio di informazioni relative a scopi istituzionali, è previsto l'uso delle liste di distribuzione (mailing list), personali o centralizzate. L'utente può avvalersi di liste di distribuzione personali, per le proprie necessità funzionali, a fronte di esigenze tecniche e/o gestionali. Una lista generale di distribuzione, centralizzata e comprendente tutti gli utenti, è gestita dal Referente ICT.
  Oltre alla lista generale di distribuzione, sono possibili altre liste centralizzate (o gruppi) utili a soddisfare le esigenze di categorie omogenee di utenti (es. Personale interno, Dirigenti, Consiglieri, etc..); l'attivazione di questi gruppi è a cura del Referente ICT che valuterà, di volta in volta, le specifiche richieste.

- Si fa presente che l'utilizzo di tali liste permette l'accesso ai messaggi da parte di tutti gli iscritti alla lista di distribuzione collegata a quell'indirizzo. Per tale motivo, sugli account sopra indicati non può essere garantita la riservatezza delle comunicazioni.
  Le informazioni istituzionali riservate, inoltre, sono segrete e oggetto di specifica tutela e, come tali, sono sottoposte a misure di sicurezza adeguate a mantenerle segrete.
  A tal fine, pertanto, si ricorda che:
  - non è consentito l'utilizzo degli indirizzi di posta elettronica dell'Ente per la partecipazione a dibattiti, forum, newsletter o mailing list, non attinenti l'attività lavorativa;
  - non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica, handicap o stato di salute o che costituiscano comunque condotta illecita;
  - è vietato l'inoltro dei messaggi ricevuti sull'account di posta istituzionale ad altro indirizzo e-mail personale del personale dipendente;
  - è severamente vietato inviare messaggi, con allegati file con contenuti inerenti alle attività dell'Ente a destinatari che non sono in relazione con la stessa e/o non sono autorizzati a riceverli, salvo espressa autorizzazione scritta del Titolare.

4.3 Utilizzo e controlli

- E' severamente vietato inviare messaggi attraverso lo strumento dell'e-mail semplice con allegati file (o nel corpo del testo) contenenti categorie particolari di dati (c.d. dati "sensibili") o dati relativi a condanne penali o reati (c.d. dati "giudiziari").

- In conformità delle disposizioni di legge e nel pieno rispetto del principio di non eccedenza, l'Ente si riserva la facoltà di effettuare controlli circa le modalità e le finalità di utilizzo della posta elettronica, soprattutto al fine di verificare la funzionalità e la sicurezza del sistema informatico. Ciò avverrà avvalendosi della facoltà di effettuare i c.d. "controlli difensivi" (attraverso soggetti all'uopo preposti), che saranno effettuati saltuariamente e/o a campione e solo in caso di stretta necessità, sull'intera area del traffico dati della posta elettronica dell'Ente ed esclusivamente per finalità di difesa e tutela del patrimonio e della sicurezza della struttura titolare del trattamento. A tal fine e per esigenze tecniche o di manutenzione, gli amministratori di sistema possono trovarsi ad avere accesso ai contenuti delle email istituzionali (in ogni caso non saranno effettuate verifiche massive, prolungate e/o indiscriminate).

  N.B.: L'Ente fa presente al personale dipendente che il servizio di posta elettronica fornito mediante l'attribuzione di un account istituzionale è uno "strumento di lavoro", al pari degli altri servizi della rete istituzionale, fra cui anche il collegamento a determinati siti internet. Costituiscono parte integrante di questi strumenti, anche i sistemi e le misure – in uso presso l'Ente - che ne consentono il fisiologico e sicuro funzionamento al fine di garantire un elevato livello di sicurezza della rete messa a disposizione del lavoratore (ad esempio: sistemi di logging per il corretto esercizio del servizio di posta elettronica; sistemi di filtraggio anti-virus che rilevano anomalie di sicurezza nelle postazioni di lavoro o sui server per l'erogazione dei servizi di rete; sistemi di inibizione automatica della consultazione di contenuti in rete inconferenti rispetto alle competenze istituzionali, senza registrazione dei tentativi di accesso).

- Salvo quanto sotto indicato, in nessun caso verrà effettuato l'accesso diretto alle caselle di posta elettronica in uso al personale dipendente, se non in seguito a gravi e comprovati motivi che possano rilevare il compimento di reati o condotte illecite oppure su segnalazione dell'Autorità Giudiziaria nell'ambito di indagini svolte per la repressione, accertamento e prevenzione di reati. In caso di un eventuale accesso all'account di posta elettronica concesso in uso al personale dipendente, i dati dei terzi saranno tutelati e l'identità degli interlocutori del lavoratore non sarà rivelata (nemmeno in eventuali sedi giurisdizionali).

- Il Personale e l'Utente, eventualmente, potrà richiedere la possibilità di utilizzare un account di posta elettronica privata, per le comunicazioni di carattere personale; in ogni caso, l'Ente si riserva il diritto di concedere o meno tale privilegio a seconda della effettiva necessità.

- Nel caso di assenza programmata e al fine di non interrompere, né rallentare i processi produttivi e/o lavorativi, il personale dipendente ha la facoltà di predisporre la funzionalità che permette l'invio di un messaggio automatico di risposta che segnali altro nominativo e relativo indirizzo di posta

elettronica di un collega da contattare nel caso di urgenze; il delegato potrà in questo modo ricevere i messaggi di posta elettronica del dipendente assente e a lui indirizzati.
Si dispone, inoltre, che nel messaggio automatico di risposta siano evidenziati l'inizio e la fine del periodo di assenza del dipendente, secondo il seguente modello:
"*Sarò assente dal___al___Per urgenze, contattare il/la sig./sig.ra ____al n. ____o all'indirizzo e-mail _____* ".

- Un utente interno può nominare una persona di fiducia che, in caso di una sua assenza, può avere accesso alla sua casella di posta al fine di garantire la continuità dell' attività lavorativa. In mancanza di questa nomina e in caso di assenza improvvisa o prolungata del dipendente, se è necessario conoscere il contenuto di messaggi di posta elettronica inviati all'indirizzo istituzionale o nel caso di motivi di manutenzione o urgenza, il rispettivo dirigente sarà legittimato a chiedere al Referente ICT di accedere alla casella di posta elettronica del lavoratore assente.

- Il personale dipendente è tenuto a visualizzare i contenuti della casella e-mail assegnata, con frequenza almeno giornaliera (durante le proprie giornate lavorative) e a usare tale strumento per qualsiasi comunicazione interpersonale nell'ambito delle finalità lavorative. Le informazioni trasmesse, molto spesso, possono o devono essere condivise, per cui deve essere salvaguardata l'integrità e la confidenzialità dei messaggi e dei contenuti.

- È fatto divieto in ogni caso di divulgare a soggetti non autorizzati le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal dovere di segretezza a cui sono tenuti i dipendenti, in ottemperanza agli obblighi di fedeltà e correttezza.

- Tutti i messaggi di posta elettronica (inviati e ricevuti), i cui contenuti possono avere una rilevanza giuridica e istituzionale per l'Ente, costituiscono corrispondenza (disciplinata dalle norme del Codice Civile e, in particolare, in base al combinato disposto degli articoli 2214 e 2220) e pertanto saranno protocollati e conservati nel protocollo informatico, secondo i tempi e i piani di conservazione e scarto predisposti dall'Ente. In ogni caso, il tempo di conservazione dei messaggi di posta elettronica, anche per le altre tipologie documentali, non sarà superiore a quello necessario agli scopi che si intendono perseguire (e, per tale motivo, può variare anche in base al ruolo a cui l'account era stato assegnato), nel rispetto dei principi di finalità, pertinenza e non eccedenza previsti dalla normativa in materia di protezione dei dati.

- Al termine della collaborazione lavorativa con l'Ente, l'eventuale account nominativo di posta elettronica istituzionale del dipendente (di proprietà dell'Ente) sarà disattivato entro 30 giorni e lo stesso Ente potrà disporre del suo utilizzo futuro, limitatamente alla corrispondenza intercorsa che ha un valore istituzionale perché attinente all'attività lavorativa del dipendente cessato (che verrà conservata per un periodo di tempo congruo rispetto agli scopi che si intendono perseguire, che può variare anche in base al ruolo e alla figura a cui l'account era stato assegnato); un messaggio automatico sull'account del dipendente cessato potrà segnalare ai mittenti il reindirizzamento dell'e-mail ad altro dipendente (su di un account alternativo). Inoltre, una volta divenute effettive le dimissioni, o in caso di licenziamento, o pensionamento, non sarà possibile inviare mail verso l'esterno, a meno di una deroga concessa dall'Ente.

5. Navigazione in Internet

- La finalità dell'accesso e della navigazione su Internet è il reperimento di informazioni e di documentazione utili all'Ente; l'utilizzo dei servizi di rete per scopi non inerenti ai fini istituzionali è consentito limitatamente alla pausa lavorativa e nel rispetto delle leggi e dei regolamenti vigenti. Non saranno normalmente esercitati controlli in relazione alla navigazione effettuata in tale lasso temporale, salvo in caso di segnalazione o richieste da parte di Autorità competenti preposte alla prevenzione di illeciti informatici.

- Durante il resto della giornata lavorativa è fatto divieto ai dipendenti di navigare in siti non attinenti con l'attività lavorativa (così come meglio descritti nell'Allegato A al presente Regolamento), in quanto l'utilizzo al collegamento ad Internet deve essere funzionale all'attività espletata in favore dell'Ente; una violazione di tale prescrizione - e qualora vengano perpetrati eventuali illeciti nella navigazione in internet - potrebbe comportare sanzioni disciplinari a carico del contravventore attraverso le modalità e le procedure in seguito indicate al paragrafo "Controlli indiretti".

- Al fine di garantire la sicurezza dei propri dati, nonché di favorire un utilizzo corretto dello strumento Internet, il Titolare potrebbe adottare alcuni accorgimenti tecnici per prevenire illeciti da parte del personale dipendente (è facoltà dell'Ente, infatti, implementare delle "black list" di siti Internet aventi l'obiettivo di impedirne la visione in quanto non ritenuti d'interesse istituzionale). Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, l'Ente adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure indicate al paragrafo "Controlli indiretti".

- L'Ente, al fine di prevenire determinate operazioni non consentite, ha implementato dei sistemi di filtro della navigazione che puntano a mitigare i rischi sopra esposti; ciononostante la prima e più efficace misura di sicurezza è rappresentata dalla consapevolezza dell'utente. Nel caso in cui un evento dannoso o una situazione di pericolo non siano stati impediti con preventivi accorgimenti tecnici, l'Ente adotterà eventuali misure che consentano la verifica di comportamenti anomali, attraverso le modalità e le procedure di seguito specificate:
  - al fine di verificare la funzionalità, la sicurezza del sistema ed il suo corretto utilizzo, le apparecchiature di rete preposte al collegamento verso internet, memorizzano un file di log contenente le informazioni relative ai siti che i PC hanno visitato. Tale archivio memorizza l'indirizzo fisico delle postazioni di lavoro e non i riferimenti dell'utente, garantendo in tal modo il suo anonimato[U1]. L'accesso a questi dati è effettuato dalla Direzione Generale e dal Referente ICT ed eventualmente da personale tecnico esterno autorizzato dalla Direzione Generale.
  - l'Ente ha attivato tali sistemi secondo le previsioni di cui al Provvedimento del Garante in materia di trattamento dati personali, (Provvedimento del 1° marzo 2007), effettuando monitoraggio generalizzato ed anonimo dei log di connessione. Pertanto, in seguito all'eventuale rilevamento di anomalie nel sistema dei dati, per motivi di manutenzione o in caso di eventuali comportamenti anomali individuati in una determinata area o a seguito di controlli a campione saltuari, l'Ente potrà attivare meccanismi di monitoraggio delle attività di rete (file di log) e di controllo del traffico internet o del traffico della posta elettronica o dei file di backup, per fini organizzativi o di manutenzione, per verifiche sulla funzionalità del sistema o di controllo della sicurezza dell'impianto. Gli archivi di log risultanti da questo monitoraggio, relativi a determinate aree dell'Ente e allo stesso tempo sufficientemente grandi da garantire la riservatezza dei lavoratori, contengono traccia di ogni operazione di collegamento effettuata dall'interno dell'Ente verso Internet.
  In caso di accertata violazione definita tramite alert, la UDSINFO del CRC provvederà prontamente a segnalare all'interessato l'attività illecita riscontrata.
  In rispetto al principio di finalità, pertinenza e non eccedenza, tali log vengono tenuti negli archivi dell'Ente per il e può accedere a tali informazioni solo il personale autorizzato o il Referente ICT. L'eventuale prolungamento dei suddetti tempi di conservazione é eccezionale e può avere luogo solo in relazione all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria oppure all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria.

- Al fine di evitare il grave rischio di importazione di virus informatici e di pregiudizio alla stabilità delle applicazioni dell'elaboratore, non è consentita l'autonoma installazione di programmi provenienti dall'esterno. Analogamente, non è possibile effettuare il download di file o di software aventi particolari caratteristiche tecniche e/o dimensionali, tali da ridurre l'efficienza e/o la sicurezza del sistema. Qualora, a seguito di controlli effettuati saltuariamente e a campione sul PC in uso all'utilizzatore, risultino presenti file o software non espressamente autorizzati, saranno posti in essere richiami disciplinari, motivati dal fatto che qualsiasi file o programma estraneo a quelli contenuti e autorizzati può cagionare incompatibilità con i programmi forniti e già in uso per lo svolgimento dell'attività lavorativa e/o costituire una minaccia per la sicurezza informatica. Il Titolare, peraltro, ricorda, all'utilizzatore, che costituiscono illecito penale le condotte consistenti nella illecita duplicazione o riproduzione di software ai sensi della legge sul diritto d'autore n. 633/41 come novellata, art. 171 bis.

- Non è permessa la partecipazione, per motivi non lavorativi, a forum, né l'utilizzo di chat line, di bacheche elettroniche, mailing list e/o altri mezzi di comunicazione telematica non attinenti con l'attività lavorativa, attuate mediante il PC affidato in uso.

5.1 Rete Dati

- E' vietato collegare, alla rete dati istituzionale, strumenti elettronici che non siano stati autorizzati;

- il computer in dotazione non deve possedere o disporre di altri collegamenti esterni diretti;
- è vietato installare mezzi di comunicazione propri;
- utilizzare esclusivamente le installazioni messe a disposizione dall'Ente ovvero quelle che siano oggetto di specifica autorizzazione;
- non usare mai la propria coppia di credenziali (utente e password) per registrarsi e/o accedere sistemi esterni;
- ricordarsi che l'Ente può monitorare il lavoro svolto e le connessioni, potendo verificare quali siti siano stati visitati e quali operazioni di trattamento sono svolte con i dati personali, di cui è titolare l'Ente;
- non inviare informazioni confidenziali tramite internet o altre reti di comunicazione elettronica senza aver preso le dovute precauzioni e aver adottato le misure di sicurezza idonee a ridurre i rischi di accesso abusivo dei dati trasmessi.

6. Utilizzo di telefoni, cellulari, fotocopiatrici e stampanti. Divieto fax.

- In generale, è opportuno non fornire indicazioni relative allo stato di salute degli utenti via telefono, se non si è certi dell'identità dell'interlocutore che sta chiamando; occorre verificare comunque che l'interessato abbia autorizzato la comunicazione dei propri dati a terzi.

- In alcuni casi, specie per chiamate di natura istituzionale (ad es. da strutture ospedaliere, autorità giudiziaria, soggetti pubblici), si consiglia di farsi lasciare dal chiamante il proprio nominativo e il numero di telefono; si provvederà a ricontattare l'ente chiamante, chiedendo della persona che ha lasciato il proprio nominativo, previa verifica dell'indispensabilità dei dati richiesti rispetto alla finalità dell'utilizzo dichiarato e della previsione normativa o dell'autorizzazione dell'interessato alla comunicazione dei propri dati.

- Non deve essere usato il fax per le comunicazioni tra l'Ente e altri Enti Pubblici poiché l'articolo 14 "Misure per favorire la diffusione del domicilio digitale", del c.d. Decreto del Fare (in seguito alle modificazioni apportate dalla legge di conversione n. 98 del 9 agosto 2013) ha stabilito che, ai fini della verifica della provenienza delle comunicazioni, è in ogni caso esclusa la trasmissione di documenti a mezzo fax. In particolare, è vietato l'uso del fax nelle trasmissioni di documenti con altre Pubbliche Amministrazioni ai sensi dell'art. 47 del Codice dell'Amministrazione Digitale;

- Non deve parimenti essere usato il fax per le comunicazioni tra l'Ente e gli enti privati o i cittadini, non costituendo obbligo nel nostro ordinamento ma solo facoltà, in tal modo favorendo un migliore andamento amministrativo e organizzativo dell'Ente medesimo.

- I telefoni, gli eventuali cellulari assegnati e le multifunzioni di piano devono essere utilizzati per scopi puramente lavorativi.

- Non è consentito rivelare numeri telefonici interni e/o informazioni sull'Ente a persone non preventivamente identificate, nonché autorizzate a conoscerle, ed è fatto divieto di lasciare documenti incustoditi presso le postazioni o presso i locali delle multifunzioni di piano. Ogni comportamento scorretto potrà anche essere oggetto di specifiche sanzioni disciplinari che potranno variare a seconda della gravità.

- Se proprio necessario, la stampa su carta di documentazione contenente dati personali e sensibili deve avvenire ad opera di personale autorizzato a trattare tali dati; inoltre, occorre ritirare tempestivamente la documentazione dalla stampante utilizzata (il riutilizzo di fogli recanti una stampa su una sola facciata, per esigenze di risparmio e di sensibilità ambientale, deve riguardare esclusivamente supporti nella esclusiva disponibilità dell' incaricato ed essere utilizzati nell' ambito delle proprie mansioni, evitando di far conoscere a terzi non autorizzati il contenuto dei documenti). I fogli contenenti dati personali e sensibili non più utilizzati e per i quali non è necessaria la conservazione, prima di essere conferiti nella raccolta differenziata, devono essere trattati in modo da rendere non intelligibili a terzi i dati personali ivi contenuti, usando un dispositivo distruggi-documenti.

7. Segreto Professionale e informazioni riservate

- Nella valutazione delle informazioni, il Personale si impegna a osservare ogni cautela perché le stesse rimangano riservate, essendo inteso che, in caso di divulgazione non autorizzata, sarà a suo carico l'onere di provare di avere adottato tali misure.
- Il Personale non può divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in tutto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni, né potrà usarle, sfruttarle o disporne in proprio o tramite terzi. Tali comportamenti includono l'inoltro di mail verso l'esterno, se non per attività lavorative e vietano altresì il re-inoltro ad altri account che non siano quelli istituzionali.
  Gli obblighi del dipendente, descritti in questo documento, non termineranno all'atto di cessazione del rapporto di lavoro.

8. Misure organizzative e di sicurezza in ambito privacy

- Ogni computer deve essere protetto da idonei strumenti per il rischio di attività di virus informatici; lo strumento di protezione (di norma, software antivirus) deve essere attivo ed è vietato disattivarlo; la posta elettronica viene filtrata in ingresso da un apposito prodotto che pulisce gli eventuali allegati contenenti virus e/o malware. Evitare comunque di aprire messaggi provenienti da mittenti sconosciuti o sospetti, e cancellarli immediatamente.

- Nel caso di utilizzo di supporti di memorizzazione esterni, controllare sempre che i file ivi memorizzati non siano infettati da virus, attraverso la scansione esplicita del supporto.

- Controllare periodicamente la presenza di virus sul proprio computer in dotazione, mediante la scansione dell'intero sistema.

- Tutto il personale dipendente che tratta dati ed è stato autorizzato al trattamento è tenuto al rispetto dei principi e delle misure organizzative e di sicurezza di cui alla normativa in materia di protezione dei dati personali; in particolare, tale personale deve:
  - trattare i dati personali secondo i principi indicati dalla legge, in modo lecito, corretto e trasparente; ciò vuol dire che deve verificare:
    i. se il trattamento sia consentito da una norma di legge o di regolamento (es. in materia di sicurezza sul lavoro o normative fiscali), o
    ii. se il soggetto i cui dati afferiscono abbia ricevuto idonea informativa e/o abbia eventualmente rilasciato il consenso (ove necessario);
  - controllare la pertinenza e non eccedenza dei dati raccolti e trattati rispetto alle finalità perseguita, evitando di accogliere dati inutili rispetto al raggiungimento della stessa (attuando il "principio di minimizzazione" nel trattamento);
  - controllare l'esattezza dei dati ed eventualmente, qualora si renda necessario, provvedere al loro aggiornamento;
  - conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi della raccolta e mettere in atto procedure tali da realizzare la cancellazione degli stessi (ovvero la loro trasformazione in forma anonima) al termine del trattamento;
  - rispettare le procedure di autenticazione informatica e di gestione delle credenziali di autenticazione predisposte dall'Ente;
  - rispettare le procedure adottate per garantire l'attività di backup e la custodia di copie di sicurezza, salvando i documenti nelle specifiche cartelle di rete a ciò riservate;
  - custodire in modo riservato (e, per i dati sensibili o giudiziari, in maniera separata e in archivi chiusi a chiave) le banche dati e comunque ogni documentazione raccolta nello svolgimento dell'attività lavorativa;
  - adottare cautele organizzative per garantire che tutte le persone con cui si collabora siano informate sulle regole di riservatezza adottate per proteggere i dati e seguire le istruzioni fornite per evitare abusi per negligenza, imprudenza o imperizia;
  - verificare sempre l'origine dei dati utilizzati;
  - segnalare al Referente ICT qualsiasi anomalia riscontrata sui sistemi informatici o nella qualità dei dati presenti nel proprio database;
  - attenersi alle istruzioni che sono state e che verranno impartite (mediante apposite lettere di autorizzazione) per garantire la corretta gestione dei dati stessi.

9. Gestione delle comunicazioni verbali

- Durante l'attività lavorativa, è consuetudine scambiare comunicazioni e informazioni in forma verbale, pertanto si rivela necessario tenere in considerazione i seguenti principi:
  - nel corso di conversazioni di lavoro occorre tutelare le informazioni coerentemente con il loro livello di classificazione e criticità;
  - lo scambio di informazioni concernente l'attività lavorativa deve avvenire all'interno di aree che consentano il mantenimento di adeguati livelli di riservatezza;
  - tali aree devono rimanere chiuse durante lo svolgimento di riunioni, conversazioni telefoniche, ecc., rilevanti per l'attività dell'Ente;
  - nel corso di conversazioni telefoniche, qualora non risulti strettamente necessario, è preferibile non fare ricorso al sistema "viva voce"; nel caso debba essere utilizzato tale sistema, l'interlocutore deve essere avvisato prima della sua attivazione;
  - prima di condividere verbalmente dati ed informazioni di lavoro, occorre accertarsi che la propria controparte, date le mansioni e le responsabilità assegnate, sia autorizzata a venirne a conoscenza;
  - coloro che sono stati provvisti di un telefono cellulare dell'Ente, devono cercare di garantire il massimo riserbo sulle proprie comunicazioni; ciò con particolare attenzione al caso in cui vengano ricevute telefonate in aree affollate, in special modo all'esterno della sede dell'Ente.

DOCUMENTAZIONE CARTACEA

- La documentazione cartacea viene spesso sottovalutata rispetto ai file presenti sul proprio PC. La riduzione del numero di fogli stampati rappresenta un grande obiettivo dal punto di vista della salvaguardia delle risorse naturali, ma anche un ottimo sistema per proteggere l'accidentale diffusione di informazioni. In tale direzione, il Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) prescrive, all'art. 40, l'obbligo di creazione e gestione dei documenti originali della Pubblica Amministrazione in modalità informatica.
  Si ricordano, a titolo esemplificativo, alcune misure utili a proteggere la riservatezza e la disponibilità delle informazioni in formato cartaceo:
  - fare ricorso alla stampa solo in caso di reale necessità e comunque il meno possibile;
  - in caso di stampa, ritirare immediatamente i documenti stampati;
  - non lasciare mai incustoditi, sul proprio tavolo, documenti riservati, anche in caso di assenza breve. In generale, riporli in contenitori sottochiave o distruggerli in modo sicuro quando non più utili;
  - la distruzione dei documenti in modo sicuro avviene con i "raccoglitori di carta" o strappandoli in piccoli pezzi. Evitare in ogni caso di gettare i documenti interi nel cestino dei rifiuti o del riciclo;
  - i documenti devono essere controllati e custoditi dagli utilizzatori fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate negli appositi archivi;
  - al termine della giornata lavorativa la propria postazione di lavoro deve essere sgombra da tutti i documenti di tipo riservato e da quelli ad uso interno nel caso il posto di lavoro non si trovi in un'area riservata al proprio dipartimento.

CONTROLLI INDIRETTI

1. Controlli

- L'Ente si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli difensivi e/o indiretti - mirati e non massivi - che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici alle presenti prescrizioni, mediante l'ausilio di personale tecnico interno o esterno appositamente autorizzato. I controlli possono scaturire anche dall'inefficienza dimostrata dal dipendente nello svolgimento della propria attività lavorativa.

La verifica circa il rispetto del presente Regolamento sarà effettuata anche attraverso gli "strumenti" affidati al personale dipendente per rendere la prestazione lavorativa e per esclusive finalità organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente e della riservatezza degli interessati. Le informazioni raccolte potranno essere utilizzate per tutte le finalità connesse al rapporto di lavoro e – nel caso di comportamenti contrari a quanto indicato nel presente Regolamento - essere utilizzate anche per l'applicazione di eventuali provvedimenti disciplinari. Per strumenti di lavoro si intende – a titolo esemplificativo - l'utilizzo di internet, della mail, del cellulare/tablet istituzionale (per verifica degli accesi internet, della posta elettronica, etc.).
Il Referente ICT, nel caso sia necessario procedere a un controllo su incarico del Titolare e per garantire la piena sicurezza della Rete o per motivi di manutenzione, si riserva di superare ogni accesso e limitazione predisposta (ad esempio password) su computer, account e-mail, dischi di rete, server, etc.

- Le verifiche di eventuali situazioni anomale avverranno attraverso le seguenti fasi:
  - analisi aggregata del traffico di rete, riferito all'intera struttura lavorativa o a sue aree (Direzione generale, Unità dirigenziale, Ufficio, etc.) e rilevazione della tipologia di utilizzo (e-mail, file, accesso a risorse estranee alle mansioni);
  - emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti alla struttura/ ufficio in cui è stata rilevata l'anomalia;
  - in caso di successivo permanere di una situazione non conforme, é possibile effettuare controlli circoscritti su singole postazioni di lavoro.

  Con la stessa gradualità, vengono effettuati controlli sull'occupazione dello spazio di memorizzazione sui server istituzionali attraverso le seguenti fasi:
  - analisi aggregata dei dati memorizzati sui server a livello di intera struttura lavorativa (Direzione generale, Unità dirigenziale, Ufficio, etc.) e rilevazione della tipologia di utilizzo (file audio, file video, immagini, software non autorizzato) e relativa pertinenza con l'attività lavorativa;
  - emanazione di un avviso generalizzato relativo ad un riscontrato utilizzo anomalo degli strumenti istituzionali, con l'invito ad attenersi scrupolosamente ai compiti assegnati ed alle istruzioni impartite; il richiamo all'osservanza delle regole può essere circoscritto agli operatori afferenti alla struttura/ ufficio in cui è stata rilevata l'anomalia;
  - in caso di successivo permanere di una situazione non conforme, è possibile procedere con un analisi puntuale ed una eventuale eliminazione del materiale non conforme, anche sulle singole postazioni di lavoro.

- Pertanto, i controlli - proporzionati e non eccedenti anche rispetto allo scopo di verifica dell'adempimento contrattuale - non potranno mai svolgersi direttamente e in modo puntuale, ma saranno preliminarmente compiuti su dati aggregati, riferiti all'intero Ente o a suoi Uffici. A seguito di detto controllo anonimo, potrà essere emesso un avviso generalizzato di rilevazione di eventuali anomalie nell'utilizzo dei presidi tecnologici e con l'invito ad attenersi scrupolosamente a compiti assegnati e alle istruzioni impartite. Se a detta comunicazione non dovessero seguire ulteriori anomalie, l'Ente non procederà a ulteriori controlli su base individuale e non saranno comunque ammessi controlli prolungati, costanti o indiscriminati. In caso contrario, verranno inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni e a, seconda della gravità della violazione perpetrata, la sanzione prevista potrà prevedere o un semplice richiamo verbale o il divieto temporaneo o permanente dell'utilizzo di strumenti informatici, sino ad arrivare alla risoluzione del rapporto di lavoro, limitatamente alle ipotesi di gravi violazioni e condotte illecite indicate nell'allegato A al presente Regolamento.

- Qualora, ad esito di controllo, il Referente ICT rilevi delle anomalie sull'utilizzo dei sopracitati strumenti informatici che possano essere configurate quali attività non conformi, provvederà ad informare il Dirigente competente. Nei casi di accertata violazione dei principi fissati nelle presenti norme generali, è prevista anche l'applicazione dei provvedimenti disciplinari come in seguito specificato, con le modalità ivi previste per il personale dipendente o equiparato e l'applicazione delle sanzioni previste nelle clausole contrattuali per i soggetti non dipendenti. L'Ente procederà altresì a segnalare l'abuso all'Autorità competente.

2. Teleassistenza

- Relativamente alle attività di manutenzione remota su PC connessi alla rete istituzionale, il personale tecnico potrà utilizzare specifici software. Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware. L'attività di assistenza e manutenzione avviene in accordo con l'utente interessato. La configurazione del software prevede un indicatore visivo sul monitor dell'utente che indica quando il tecnico è connesso al personal computer.
  Viene fornita, su richiesta, una comunicazione informativa sullo strumento utilizzato, nonché le modalità del suo utilizzo per tutti gli utenti interessati.

FORMAZIONE E AWARENESS

La prima misura di sicurezza per la protezione delle informazioni istituzionali è indubbiamente la preparazione e consapevolezza del personale dipendente nello svolgere il proprio lavoro in modo sicuro.

Consapevolezza e preparazione sono aspetti che fanno parte del background del personale dipendente ma che possono essere sviluppati anche attraverso la formazione nelle varie fasi della vita lavorativa (corsi di inserimento e richiami periodici).

Sono state previste sessioni formative e aree dedicate alla formazione. In tali aree si potranno reperire varie risorse per accrescere le proprie competenze e di riflesso migliorare la gestione delle informazioni istituzionali.

Periodicamente si procede a interventi formativi specifici per tutti coloro che trattano dati personali e che sono stati istruiti mediante lettera di autorizzazione al trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure organizzative e di sicurezza adeguate adottate dall'Ente. La formazione viene programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Il Responsabile della Protezione dei Dati personali (DPO), punto di contatto per tutto il personale dipendente e gli Utenti (interni ed esterni) per le attività che riguardano e impattano sul trattamento dei dati personali, è a disposizione per qualsiasi dubbio o segnalazione.

Si ricorda che i corsi di formazione previsti non sono facoltativi e che la ingiustificata assenza può portare a provvedimenti di tipo tecnico-disciplinare.

RESPONSABILITA'

Ogni utente è responsabile, civilmente e penalmente, del corretto uso delle Risorse Informatiche, dell'utilizzo dei servizi e programmi ai quali ha accesso e delle informazioni che tratta. L'assegnazione di risorse informatiche non ne comporta il possesso, in quanto trattasi di strumenti di esclusiva proprietà dell'Ente. Gli utenti interni utilizzano, nel proprio lavoro, soltanto strumenti informatici assegnatigli dall'Ente.

L'uso di computer privati deve essere preventivamente autorizzato dal Referente ICT.

Per motivi di sicurezza e protezione dei dati, oltre che per ottemperare alle normative vigenti, ogni attività svolta con il Sistema Informatico istituzionale è sottoposta a registrazione in appositi file (log) con riferimento alle credenziali dell'utente e alla stazione di lavoro utilizzata. Detti file possono essere utilizzati per attività di monitoraggio e controllo del buon funzionamento del Sistema Informatico da parte degli Amministratori di Sistema, e possono essere messi a disposizione dell'Autorità Giudiziaria nei casi previsti dalla normativa.

La riservatezza delle informazioni in essi contenute è soggetta a quanto dettato dal Regolamento UE 2016/679 e dal D.Lgs. 196/2003. Ciascun Dirigente ha la responsabilità di vigilare e verificare il corretto utilizzo degli strumenti informatici assegnati alla propria Direzione/Area/Osservatorio e di evitare l'uso improprio o l'accesso da parte di personale non autorizzato, richiedendo agli amministratori di sistema e tecnici dell'Ente gli eventuali interventi necessari.

SANZIONI E PROVVEDIMENTI DISCIPLINARI

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento sono perseguibili con provvedimenti disciplinari individuati nel CCNL vigente (allegato al presente Regolamento) nonché, nei casi più gravi, con azioni civili e penali. E' comunque immediatamente applicato, a scopo cautelativo, il temporaneo divieto di utilizzo di strumenti informatici.

A seconda della gravità della violazione perpetrata la sanzione disciplinare prevista può prevedere:

- un semplice richiamo verbale;
- un rimprovero scritto;
- l'applicazione della multa (nella misura determinata nel CCNL);
- la risoluzione immediata del rapporto di lavoro (giusta causa).

Prima di assumere qualsiasi decisione disciplinare per un uso non corretto degli strumenti informatici, della mail istituzionale o di internet per fini personali, tuttavia, il dipendente sarà invitato a motivare la ragione di tale utilizzo.

La non osservanza del presente regolamento e disposizioni ivi presenti può comportare, oltre alle sanzioni disciplinari, anche sanzioni civili e penali.

Si precisa inoltre che, ai fini disciplinari, le presenti disposizioni e procedure operative interne oltre a essere state pubblicate sulla Intranet dell'Ente, sono affisse in luogo accessibile a tutti (es. bacheca[U2]), ai sensi dell'art. 7 della Legge 20 maggio 1970 n. 300.

DEROGHE E MODIFICHE DEL PRESENTE REGOLAMENTO

Qualora al presente Regolamento l'Ente intenda apportare modifiche, queste saranno applicate dandone conoscenza immediata al personale dipendente mediante apposita circolare di servizio.

Qualora si renda necessario per qualsiasi motivo, derogare ad uno o più punti del presente Regolamento, salvo i casi in cui le deroghe siano espressamente previste e disciplinate nello stesso Regolamento, sarà obbligatorio porre per iscritto e veder accettata dal Personale e dall'Ente tale deroga mediante sottoscrizione di entrambe le parti.

Deroghe o modifiche di uno o più punti del presente Regolamento, non rendono invalidi gli altri punti, salvo ipotesi di evidente incompatibilità, per cui prevarrà l'applicazione della clausola temporalmente più recente.

Eventuali comportamenti non in linea con il presente Regolamento, che venissero comunque tollerati dall'Ente, non costituiscono una rinuncia dello stesso ad esercitare successivamente i suoi diritti per far valere il presente Regolamento.

Il Titolare del Trattamento
Consiglio regionale della Campania

ALLEGATO A

1) ELENCO DELLE CONDOTTE ILLECITE VIETATE E ASSOGGETTABILI A SANZIONE DISCIPLINARE, ANCHE NEGLI ESTREMI DEL LICENZIAMENTO, E LEGALMENTE PERSEGUIBILI:

a) Navigazione intenzionale all'interno di siti web pornografici o pedo-pornografici, detenzione di files di tale natura e/o loro scambio con soggetti terzi (sanzione: Licenziamento);

b) Utilizzo intenzionale della rete istituzionale ai fini di:

- creare o trasmettere qualunque immagine, dato o altro materiale offensivo, diffamatorio, osceno, indecente, o che attenti alla dignità umana, specialmente se riguardante il sesso, la razza o il credo;
- creare e conservare su sistemi e supporti informatici immagini, documenti, dati a carattere privato e non attinenti all'attività lavorativa;
- danneggiare, distruggere, cercare di accedere senza autorizzazione ai dati o violare la riservatezza di altri utenti, compresa l'intercettazione o la diffusione di parole di accesso (password) e ogni altro "dato personale" come definito dalle leggi sulla protezione della privacy (sanzione: Licenziamento);
- effettuare di qualsiasi tipo di attività volta a raggirare o compromettere i meccanismi di protezione dei sistemi informativi (sanzione: Licenziamento);
- sfruttare qualsiasi vulnerabilità derivante da difetti di configurazione o difetti intrinseci ai programmi e/o ai sistemi al fine di commettere azioni illecite o non autorizzate (sanzione: Licenziamento);
- falsificare la propria identità (sanzione: Licenziamento);
- svolgere sulla Rete ogni altra attività vietata dalla Legge dello Stato e dalla normativa Internazionale (sanzione: Licenziamento).

c) Download intenzionale da internet di files non correlati all'attività lavorativa e per i quali derivi un danno in capo all'Ente, di natura civile e/o penale, quale conseguenza della violazione degli obblighi imposti dal d.lgs. 29 dicembre 1992, n. 518, sulla tutela giuridica del *software* e/o dalla l. 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore (a titolo esemplificativo: file musicali, film o altro materiale coperto da diritti d'autore);

d) Accesso reiterato e per periodi di tempo complessivamente rilevanti a siti internet di contenuto non attinente all'attività lavorativa, anche dopo avere eventualmente ricevuto specifici richiami in materia;

e) Comunicazione della password istituzionale a terzi, senza a ciò essere stati preventivamente autorizzati, nell'ipotesi che da tale comunicazione deriva un danno all'Ente;

f) Utilizzo del telefono o del cellulare di servizio, con costi a carico dell'Ente, per scopi palesemente non istituzionali e non attinenti alla propria attività lavorativa;

g) Comunicazione/distribuzione/diffusione a terzi documenti classificati come "RISERVATI", ricevuti via mail o con altro mezzo, senza un'autorizzazione scritta del proprietario\creatore del documento\file o del Titolare del trattamento;

h) Copiare qualsiasi dato o file ovvero comunicare o diffondere all'esterno dati o file, soprattutto se "Ad uso interno" o "Riservati", in assenza di una preventiva autorizzazione.

2) ELENCO DELLE TIPOLOGIE DI SITI WEB CORRELATI ALL'ATTIVITÀ LAVORATIVA E LIBERAMENTE NAVIGABILI:

- Siti di Enti Pubblici in genere (es. Ministeri, etc.);
- Siti web di fornitori di servizi;
- Siti web di enti ed organizzazioni istituzionali.

Si rende noto che l'Ente, mediante le funzioni interne preposte, provvederà a denunciare alle autorità competenti tutti i casi di utilizzo dei sistemi informativi interni ritenuti in contrasto con la normativa vigente.

L'Ente, nella persona del proprio legale rappresentante, ha facoltà di promuovere azione di rivalsa per danni provocati dall'inosservanza del Regolamento interno o per danneggiamento delle apparecchiature informatiche.

L'utente/dipendente e ogni destinatario del Regolamento è sempre direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio Internet. La responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso.

La violazione del Regolamento interno comporta l'applicazione dei provvedimenti sanzionatori nello stesso descritti o la sospensione d'ufficio dell'utilizzo delle risorse informatiche a disposizione, fatte salve le più gravi sanzioni previste dalle norme di legge e inoltre per il personale dipendente risultano applicabili gli articoli del CCNL di riferimento e l'articolo 7 dello Statuto dei Lavoratori.

Consiglio Regionale della Campania

Procedura per l'esercizio dei nuovi diritti

GESTIONE DELLE MODIFICHE

Versione	Data emissione	Descrizione delle modifiche
1	25-05-2020	Prima versione

Indice dei contenuti

INTRODUZIONE

Il presente documento descrive i principi generali che disciplinano l'esercizio dei nuovi diritti dell'interessato (accesso, rettifica, cancellazione, limitazione) previsti dal Regolamento UE 2016/679. Descrive inoltre le competenze e le responsabilità di processo e i flussi procedurali previsti.

DESTINATARI

Il presente documento si applica al Consiglio regionale della Campania ("CRC" o "Ente") e a tutto il personale coinvolto in operazioni di trattamento (sia esso in qualità di "Designato" o "Autorizzato").
Titolare del processo è il Designato di Unità Dirigenziale o degli Organismi, che ha il compito di fornire il riscontro ufficiale all'interessato (Responsabile del riscontro).

Le altre funzioni che partecipano al processo sono il Responsabile della Protezione dei Dati (RPD o DPO), coinvolto nell'analisi dell'ammissibilità della richiesta e nella validazione finale della risposta, gli "autorizzati" (personale dipendente che tratta i dati personali oggetto della richiesta) e le funzioni IT (interne o esterne), coinvolte nell'accesso alle banche dati.

Le responsabilità sono ripartite secondo quanto indicato dalla seguente matrice RACI:

Attività	Titolare del trattamento	Designato di Unità Dirigenziale o degli Organismi (Responsabile del Riscontro)	DPO	Autorizzato	Funzioni IT
Accettazione della domanda	A	R			
Verifica della richiesta		A/R	C		
Identificazione trattamenti		A/R		C	
Identificazione dati		I		A/R	
Elaborazione dati		I		I	A/R
Risposta	A	R	C		

NORMATIVA DI RIFERIMENTO

- Regolamento UE 2016/679 - regolamento generale sulla protezione dei dati (o GDPR, General Data Protection Regulation)

PRINCIPI GENERALI

In relazione al trattamento dei propri dati personali l'interessato (cittadini, dipendenti, fornitori, consulenti, tutte in qualità di persone fisiche) ha diritto di ottenere dal Titolare del trattamento:

- La conferma che sia o meno in corso un trattamento di dati personali che lo riguardano, e di ottenere:
    - le finalità del trattamento;
    - le categorie di dati personali in questione;
    - i destinatari a cui tali dati sono stati comunicati;
    - il periodo di conservazione previsto (o i criteri utilizzati per determinare tale periodo);
- La rettifica dei dati personali che lo riguardano e l'integrazione di dati personali incompleti;
- La cancellazione, trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- La limitazione del trattamento, in caso di:
    - contestazione dell'esattezza dei dati personali, per il periodo necessario a verificare la correttezza di tali dati;
    - trattamento illecito;
    - dati necessari all'interessato per la difesa di un diritto in sede giudiziaria;
    - in attesa della verifica in merito alla richiesta di opposizione al trattamento;

L'acquisizione dei dati personali che lo riguardano per trasmetterli ad un altro titolare del trattamento.

L'interessato ha inoltre il diritto di opporsi in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano.

Il CRC, in qualità di Titolare del trattamento, ha adottato misure tecniche e organizzative per favorire l'esercizio dei diritti degli interessati e garantire il riscontro alle richieste presentate. Qualsiasi richiesta pervenuta in relazione all'esercizio dei diritti degli interessati, che non pervenga all'indirizzo di posta elettronica del Responsabile della Protezione dei Dati deve essere portata a conoscenza dello stesso Responsabile della Protezione dei Dati e del

Designato di Unità Dirigenziale o degli Organismi, nel più breve tempo possibile, da parte del personale interno che l'abbia eventualmente ricevuta.

Tutte le richieste pervenute al CRC sono protocollate e registrate in un apposito registro che riporta la data, le generalità del richiedente ed i contenuti della richiesta stessa.

In tutti i casi di presentazione di una richiesta e in assenza di strumenti informatici che possano dimostrare in maniera inequivocabile l'identità del richiedente, l'interessato viene identificato mediante una copia di un documento di riconoscimento oppure attraverso le modalità previste dall'art. 65 del D. L.vo 82/05, al fine di evitare che soggetti terzi possano abusivamente esser messi a conoscenza dei dati trattati dal CRC.

Il CRC risponde all'interessato delle richieste relative ai suoi diritti entro il termine di un mese. Tale termine è estendibile sino a tre mesi, in casi di richieste di particolare complessità. Viene dato comunque un riscontro all'interessato entro un mese dalla richiesta, anche in caso di diniego o nel caso di proroga sino a tre mesi, indicandone i motivi.

INPUT E OUTPUT DEL PROCESSO

Input	Provenienza
Richiesta di accesso/ rettifica/ cancellazione/ limitazione	Interessato

Output	Destinazione
Risposta del CRC alla richiesta dell'interessato	Interessato

DESCRIZIONE DEL PROCESSO

Il CRC, in qualità di Titolare del trattamento, ha definito il seguente processo per dare riscontro all'interessato in seguito alla presentazione di una richiesta di accesso, rettifica, cancellazione, limitazione o portabilità dei dati.

Accettazione della domanda

L'interessato invia la propria richiesta al CRC attraverso i canali indicati nell'informativa.

Se l'interessato non è un dipendente del CRC, al momento della presentazione della richiesta e salvo altri strumenti di identificazione personale previsti dal Codice dell'Amministrazione Digitale, deve allegare una copia di un documento di riconoscimento (e quindi deve essere richiesta ad integrazione della domanda se non è inizialmente prodotta), al fine di evitare che soggetti terzi possano abusivamente esser messi a conoscenza dei dati trattati dal CRC.

L'accettazione e la registrazione della richiesta viene svolta dal Responsabile del riscontro. Qualora le richieste dovessero pervenire ad altre funzioni dell'Ente, vengono inoltrate al Responsabile del riscontro e, per conoscenza, al Responsabile della Protezione dei Dati.

Tutte le richieste vengono registrate dal Responsabile del riscontro nel Registro delle richieste per l'esercizio dei nuovi diritti, riportando la data, le generalità del richiedente ed i contenuti della richiesta stessa.

Verifica della richiesta

Il Responsabile del riscontro esegue una verifica della richiesta fatta dall'interessato e consulta il DPO per una valutazione della legittimità della richiesta.

Se la richiesta non è ritenuta ammissibile, risponde all'interessato entro il termine di un mese informandolo del diniego.

Se la richiesta è ritenuta ammissibile, predispone la risposta all'interessato entro il termine di un mese. In caso di richieste di particolare complessità tale termine può essere esteso sino a tre mesi. In tal caso viene dato un riscontro all'interessato entro un mese dalla richiesta.

Predisposizione risposta

Le attività previste per la predisposizione della risposta variano in base al tipo di richiesta formulata dall'interessato.

Diritto all'accesso

Il Regolamento UE 2016/679 (art. 15) definisce il diritto di accesso dell'interessato al trattamento di dati personali come il diritto di richiedere e ottenere dal Titolare del trattamento - senza giustificato ritardo - la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano.

Per rispondere alle richieste di accesso ai dati da parte dell'interessato, il CRC ha definito il seguente sotto-processo:

<u>Responsabile del riscontro</u>

- Identificazione dei trattamenti riguardanti la richiesta dell'interessato nel Registro delle attività di trattamento;
- Coinvolgimento del Responsabile della Protezione dei Dati (DPO), dell'Autorizzato al trattamento per l'identificazione dei dati relativi alla richiesta dell'interessato, dei sistemi informativi che li trattano e il coinvolgimento - se presenti - di eventuali Responsabili esterni.

Autorizzato al trattamento

- Individuazione dei dati e predisposizione dell'accesso alle banche dati.

Responsabile Sistemi Informativi (IT)

- Recupero dei dati personali dell'interessato dalle banche dati identificate.

Responsabile del riscontro

- Predisposizione della risposta all'interessato, contenente:
  - una copia dei dati personali oggetto del trattamento che lo riguardano;
  - ulteriori informazioni rilevanti, tra cui le finalità del trattamento, le categorie di dati personali trattati, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e (ove possibile) il periodo di conservazione.

Qualora la risposta fornita dal CRC contenga anche riferimenti a terzi, i dati personali di quest'ultimi saranno cancellati (o resi anonimi) dal Responsabile del riscontro, salvo che ciò renda incomprensibili le informazioni richieste dall'interessato.

Diritto alla rettifica delle informazioni

Il Regolamento UE 2016/679 (art. 16) definisce il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e l'integrazione di dati personali incompleti.

Per rispondere alle richieste di rettifica da parte dell'interessato, il CRC ha definito il seguente sotto-processo:

Responsabile del riscontro

- Individuazione dei trattamenti riguardanti la richiesta dell'interessato nel Registro delle attività di trattamento;
- Coinvolgimento del Responsabile della Protezione dei Dati (DPO), dell'Autorizzato al trattamento per l'identificazione dei dati relativi alla richiesta dell'interessato e dei sistemi informativi che li trattano;

Autorizzato al trattamento

- Individuazione dei dati e predisposizione della rettifica o integrazione.

Responsabile Sistemi Informativi (IT)

- Aggiornamento o integrazione delle informazioni indicate dall'interessato nelle banche dati identificate.

Diritto di cancellazione (diritto all'oblio)

L'art. 17 del Regolamento UE 2016/679 prevede l'esistenza del diritto per l'interessato di ottenere la cancellazione dati personali che lo riguardano e che sono nella disposizione del titolare del trattamento (diritto all'oblio).

Per rispondere alle richieste di accesso ai dati da parte dell'interessato, il CRC ha definito il seguente sotto-processo:

Responsabile del riscontro

- Individuazione dei trattamenti riguardanti la richiesta dell'interessato;
- Coinvolgimento del Responsabile della Protezione dei Dati (DPO), dell'Autorizzato al trattamento per verificare la sussistenza di uno dei seguenti casi:
  - i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati;
  - l'interessato ha revocato il consenso su cui si basa il trattamento;
  - non sussiste altro fondamento giuridico per il trattamento;
  - non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
  - i dati personali sono stati trattati illecitamente.

In caso affermativo:

Autorizzato al trattamento

- Individuazione dei dati e predisposizione delle attività di cancellazione.

Responsabile Sistemi Informativi (IT)

- Cancellazione dei dati indicati dalle banche dati identificate.

Diritto di limitazione del trattamento

L'art. 18 del Regolamento UE 2016/679 prevede il diritto di limitazione del trattamento, esercitabile dall'interessato in caso di violazione dei presupposti di liceità del trattamento (in alternativa alla cancellazione dei dati), o nel caso in cui l'interessato chieda la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si opponga al loro trattamento ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

In caso di richiesta di limitazione del trattamento, ogni altro trattamento tranne la conservazione del dato è vietato, a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Per rispondere alle richieste di limitazione del trattamento, il CRC ha definito il seguente sotto-processo:

Responsabile del riscontro

- Individuazione dei trattamenti riguardanti la richiesta dell'interessato nel Registro delle attività di trattamento;
- Coinvolgimento del Responsabile della Protezione dei Dati (DPO), dell'Autorizzato al trattamento per verificare la sussistenza di uno dei seguenti casi:
  - il trattamento è illecito e l'interessato ha chiesto la limitazione in alternativa alla cancellazione dei dati personali;
  - l'interessato contesta l'esattezza dei dati personali e ha chiesto una rettifica;
  - l'interessato si è opposto al trattamento ed è in attesa delle verifiche necessarie per determinare se i motivi legittimi del titolare del trattamento prevalgano su quelli dell'interessato;
  - i dati sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, mentre al titolare del trattamento non servono più a fini del trattamento.

Autorizzato al trattamento

- Individuazione dei dati per i quali si richiede la limitazione del trattamento

Responsabile Sistemi Informativi (IT)

- Marcatura dei dati per i quali si richiede la limitazione rendendoli inaccessibili agli utenti (o in alternativa trasferimento temporaneo dei dati selezionati verso altri sistemi) in attesa di determinazioni ulteriori.

Diritto di opposizione

L'art. 21 del Regolamento UE 2016/679 prevede il diritto di opposizione, che permette agli interessati di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni.
In tali casi, il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Per rispondere alle richieste di limitazione del trattamento, il CRC ha definito il seguente sotto-processo:

Responsabile del riscontro

- Individuazione dei trattamenti riguardanti la richiesta dell'interessato nel Registro delle attività di trattamento;
- Coinvolgimento del Responsabile della Protezione dei Dati (DPO), dell'Autorizzato al trattamento per verificare la sussistenza di un motivo legittimo dell'interessato per l'opposizione.

Autorizzato al trattamento

- Individuazione dei dati per i quali si richiede l'opposizione al trattamento.

Responsabile Sistemi Informativi (IT)

- Individuazione dei dati per i quali si richiede l'opposizione e implementazione delle eventuali azioni per terminare l'attività di trattamento.
- Aggiornamento della volontà dell'interessato (es. revoca del consenso) e individuazione dei dati per i quali si richiede l'opposizione.

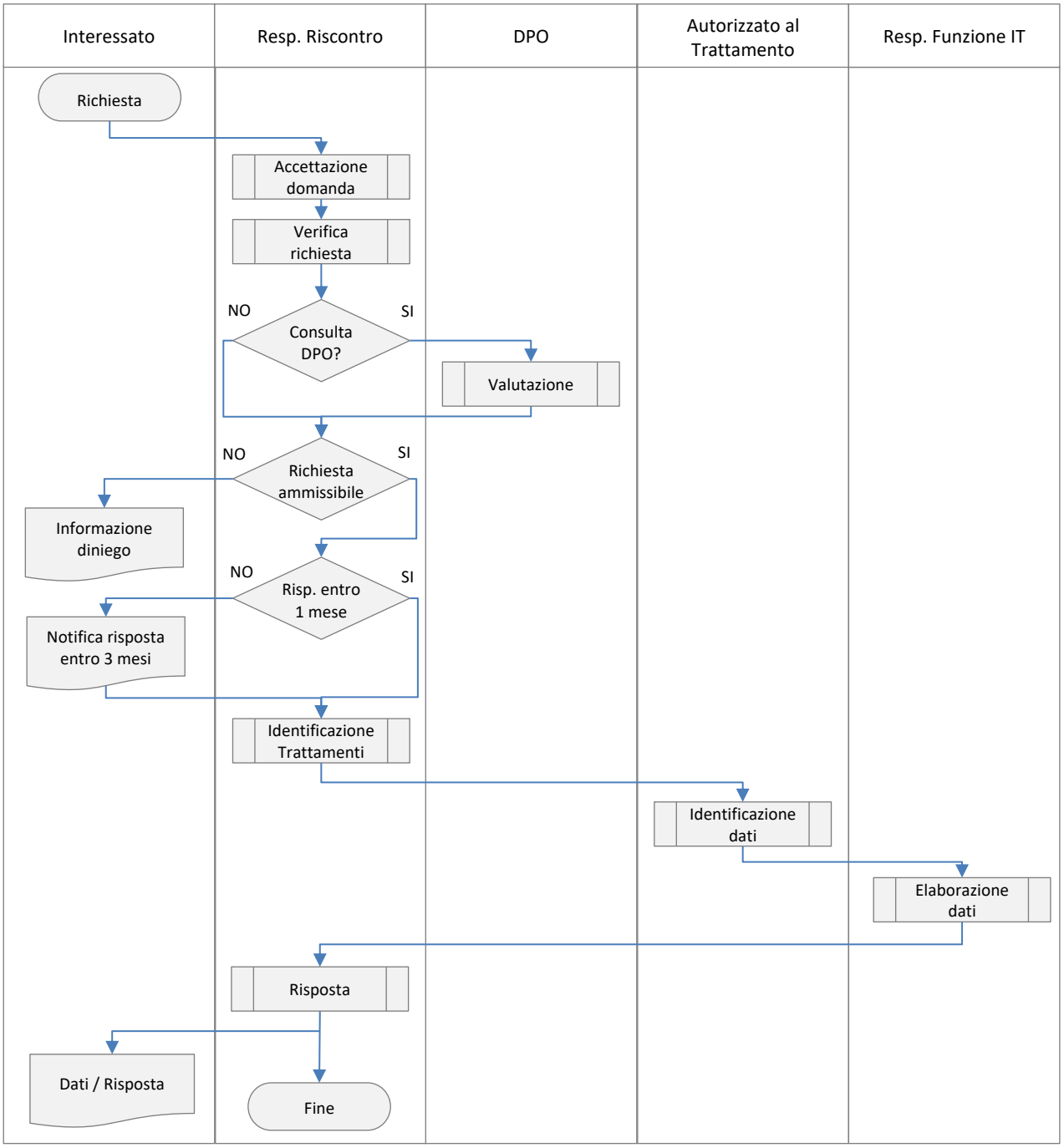
Risposta

Il Responsabile del riscontro predispone la risposta all'interessato indicando l'esito delle attività svolte e allegando i dati richiesti ove previsti (diritto di accesso e diritto di portabilità).

La risposta viene firmata dal Responsabile del riscontro per certificare la qualità delle operazioni svolte sui dati e dal DPO, a garanzia della conformità al presente processo.

Il Responsabile del riscontro invia la risposta all'interessato nel rispetto dei tempi attraverso i canali predisposti dal CRC ed indicati nell'informativa, aggiorna il registro e archivia la risposta alla pratica relativa alla richiesta.

FLUSSO DI GESTIONE



DESCRIZIONE RUOLI

Di seguito viene riportata una descrizione dei ruoli indicati nella matrice RACI per le funzioni coinvolte nelle attività del processo:

- **Responsible (R):** È responsabile dell'esecuzione dell'attività. Per un'attività deve esistere almeno un responsabile;

- **Accountable (A):** Ha la responsabilità generale dei risultati di un'attività. Conseguentemente è tenuto a rispondere della misura in cui sono stati raggiunti gli obiettivi e di quali aspettative sono state soddisfatte. Per un'attività deve essere presente un unico soggetto accountable;
- **Consulted (C):** Partecipa alla realizzazione di un'attività o contribuisce, a vario titolo, alla produzione di contributi informativi attesi. Può trattarsi di una persona consultata per un parere o per svolgere una specifica sotto-attività in qualità di esperto. In quest'ultimo caso, il suo coinvolgimento è generalmente limitato nel tempo. Per un'attività possono essere presenti più enti/ruoli che collaborano;
- **Informed (I):** È informato dell'esecuzione di un'attività avendone un interesse specifico. Per un'attività possono essere presenti più enti/ruoli informati.

ALLEGATI

- **Registro delle richieste per l'esercizio dei nuovi diritti**

Il Titolare del Trattamento

Consiglio regionale della Campania

Compilazione a cura del RPD / Designato / Autorizzato / Responsabile				
Segnalazione	**N°**	**Data**		
Rilevazione a seguito di:	❑ **Incidente**	❑ **Terzi**	❑ **Audit interno**	❑ **Altro**

Dati del segnalatore

Nome	
Cognome	
Area appartenenza/esterno	
Indirizzo PEC o e-mail per eventuali comunicazioni	
Recapito telefonico	

Segnalazione incidente

Descrizione dell'incidente (cosa è successo)	
Modalità dell'incidente (come è successo)	
Cause dell'incidente (perché è successo)	
Come è stato rilevato l'incidente	
Sistemi e supporti interessati	
Aree o uffici interessati	
Evidenze oggettive allegate	

Modello compilato da	
Segnalato al *Titolare/ DPO / Responsabile Unità Dirigenziale*	***Data***

Titolare del trattamento

Denominazione				
Indirizzo	*Prov.*		*Comune*	
	Cap		*Indirizzo*	
Persona addetta alla comunicazione				
Funzione rivestita				
Indirizzo PEC o e-mail per eventuali comunicazioni				
Recapito telefonico				

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati?

[ ] Il giorno _____

[ ] Tra il _____ e il _____

[ ] In un tempo non ancora determinato

[ ] E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

a) Tipo di violazione

[ ] Lettura (presumibilmente i dati non sono stati copiati) (Riservatezza)

[ ] Copia (i dati sono ancora presenti sui sistemi del titolare)

[ ] Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

[ ] Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

[ ] Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

[ ] Altro:

b) Dispositivo oggetto della violazione

[ ] Postazione di lavoro / computer

[ ] Rete

[ ] Dispositivo mobile

[ ] File o parte di un file

[ ] Strumento di backup

[ ] Documento cartaceo

[ ] Altro:

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

Quali categorie di interessati ha riguardato la violazione di dati?

[ ] Dipendenti
[ ] Minori/Genitori
[ ] Cittadini / Consumatori
[ ] Altro specificare: ……
[ ] Altro specificare: ……

Quante persone sono state colpite dalla violazione di dati?

[ ] Nr. _____ di persone
[ ] Circa _____ persone
[ ] Un numero (ancora) sconosciuto di persone

Quante registrazioni sono state interessate dalla violazione di dati?

[ ] Nr. _____ di registrazioni
[ ] Circa _____ registrazioni
[ ] Un numero (ancora) indeterminato

Altri dati coinvolti nella violazione

[ ] Dati anagrafici / codice fiscale
[ ] Dati di accesso e di identificazione (user name, password, customer ID, altro)
[ ] Dati relativi a minori
[ ] Dati personali idonei a rivelare lo stato di salute e la vita sessuale
[ ] Dati giudiziari
[ ] Copia per immagine su supporto informatico di documenti analogici
[ ] Ancora sconosciuto
[ ] Altro:

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

[ ] Basso / Trascurabile [ ] Medio [ ] Alto [ ] Molto alto

Misure tecniche ed organizzative applicate ai dati colpiti dalla violazione

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

Valutazione dei rischi conseguenti l'evento per i diritti e le libertà degli interessati, tenendo in considerazione le misure preventive attuate per far fronte ai danni

[ ] NON PRESENTI [ ] PRESENTI [ ] ELEVATI

Natura della comunicazione

[ ] Nuova comunicazione

[ ] Inserimento ulteriori informazioni sulla precedente comunicazione (numero di riferimento) _____

La violazione è stata comunicata anche agli interessati?

[ ] Sì, è stata comunicata il _____

[ ] Si sta provvedendo ad effettuare la comunicazione nelle prossime ore

[ ] No, perché _____

La violazione coinvolge interessati che si trovano in altri Paesi UE?

[ ] Sì [ ] No

La comunicazione è stata effettuata alle competenti autorità di controllo?

[ ] No, perché _____

[ ] Sì

Numero incidente	Data evento	Descrizione evento	Rimedi	Notifica interessati?	Notifica Autorità?	Note

Comunicazione della Violazione dei Dati personali (Data Breach) ai soggetti interessati

Gentile *Dipendente/Fornitore/Visitatore*,

il Consiglio regionale della Campania è molto attento alla tutela dei dati personali ed attua una serie di misure di sicurezza, tecniche ed organizzative per proteggerli.

Ciononostante, si è verificato un incidente che potrebbe mettere a rischio la sicurezza dei dati che La riguardano e per limitare al massimo gli effetti di questo incidente, stiamo lavorando per contenerne gli effetti.

Al tempo stesso, vogliamo renderLa partecipe dell'accaduto e fornirLe ogni indicazione possibile nonché alcuni consigli per evitare ulteriori conseguenze.

Le riportiamo di seguito il nominativo del Responsabile Protezione Dati che potrà contattare nel caso avesse bisogno di ulteriori informazioni o istruzioni in merito alle azioni che si dovessero rendere necessarie.

Responsabile Protezione Dati (eventualmente da contattare per informazioni sul Data Breach)

Cognome e Nome				
	Prov:		Comune	
	Cap		Indirizzo	
Indirizzo PEC o e-mail per eventuali comunicazioni				
Recapito telefonico				

Descrizione della natura della violazione dei dati personali

L'incidente si è verificato:

[ ] Il giorno _____
[ ] Tra il _____ e il _____
[ ] In un tempo non ancora determinato
[ ] E' possibile che sia ancora in corso

Probabili conseguenze della violazione dei dati personali

Quali misure di sicurezza sono state adottate preventivamente o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

Cosa fare per contenere gli effetti della violazione

Restiamo a disposizione per ogni chiarimento si rendesse necessario, rassicurandoLa sin d'ora che il Consiglio regionale della Campania sta già lavorando per risolvere l'increscioso incidente.

Consiglio Regionale della Campania

ALLEGATO A:

ISTRUZIONI OPERATIVE PER I DIPENDENTI AUTORIZZATI A TRATTARE I DATI PERSONALI

AI SENSI DEL REGOLAMENTO UE 2016/679 "GENERAL DATA PROTECTION REGULATION"

Data Creazione	Verificato da:	Approvato da:	Note
25-05-2020	Giuseppe Ferretti	Giovanna Donadio	Revisione 1

Sommario

Istruzioni e regole per il trattamento di dati con l'ausilio di strumenti elettronici

Tutto il personale che partecipa ai trattamenti (personale, interno ed esterno, autorizzato dal **Titolare**) che, a qualunque titolo accede, al Sistema informativo, che si trovi all'interno della rete informatica, collegato o meno a tale rete, o che custodisce qualsiasi dato personale (anche cartaceo) di competenza del **Titolare** e non destinato alla diffusione, dovrà attenersi a quanto riportato di seguito. In particolare, si evidenzia che:

- L'accesso a un qualunque tipo di trattamento di dati personali con strumenti elettronici è sempre subordinato al superamento di una procedura di autenticazione informatica, che prevede l'inserimento di un codice di identificazione personale (username) e di una password (**password**) riservata e conosciuta solamente dal medesimo utilizzatore.
- L'accesso a ulteriori livelli di strumenti informatici, necessari per il trattamento di dati personali per una corretta esecuzione del proprio incarico, è garantito dalla configurazione, sul proprio profilo, di ulteriori livelli di credenziali di autenticazione.
- Il personale autorizzato deve tenere presente che la password rappresenta la prima barriera in una strategia di accesso selettivo a dati personali, e pertanto una password costruita con criteri non soddisfacenti può portare alla compromissione dell'intera rete informativa.

Per queste ragioni, ciascuno **è responsabile della segretezza della password associata al proprio codice di identificazione (nome utente o userid) ed è tenuto a prendere tutte le iniziative appropriate per garantire la sicurezza della stessa**.

Pertanto, è indispensabile che tutto il personale prenda buona nota di quanto appresso illustrato e che si attenga strettamente a queste indicazioni.

Linee guida per la costruzione delle password

Premessa: in CRC ogni utente è censito individualmente e registrato sul dominio Windows del CRC, per cui, per poter accedere a qualsiasi PC o applicazione, anche da remoto, l'utente deve essere in possesso di una coppia di credenziali (account e password).

La regola per gli account, indicata dal **Responsabile ICT**, è la seguente:

<cognome.3lettereinizialidelnome@cr.campania.it>

Le regole per le password, indicate dal **Titolare,** prevedono quanto segue.

Password per l'accesso all'ambiente Windows.

- definizione della password al primo accesso dell'utente, dopo l'attivazione o riattivazione del proprio account.

- password nota SOLO all'incaricato, che ha la facoltà di cambiarla autonomamente in qualsiasi momento.
- composta da almeno 10 (dieci) caratteri
- contenente caratteri scelti in almeno 3 delle seguenti categorie:
    - lettere maiuscole (da A a Z)
    - lettere minuscole (da a a z)
    - numeri (da 0 a 9)
    - caratteri non alfanumerici (ad esempio: !, $, #, %)
- non contenente riferimenti agevolmente riconducibili all'utilizzatore
- cambiamento della password ogni **6 mesi** per gli account autorizzati al trattamento di dati comuni
- cambiamento della password ogni **3 mesi** per gli account autorizzati al trattamento delle categorie particolari di dati
- la nuova password impostata dall'utente non potrà essere uguale a quella in scadenza ovvero alle ultime quatto (4) utilizzate.

Password per l'accesso ad ulteriori livelli di applicativi.

Per gli eventuali ulteriori livelli di applicativi che prevedono l'inserimento di password, occorre attenersi, laddove possibile, alle regole sopra citate.

Password sicure.

Si riportano alcune indicazioni per aiutare nella scelta di password che possono considerarsi sicure.

Sono da ritenere password di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- non devono rappresentare una "parola" in una qualsiasi lingua o dialetto sufficientemente diffuso
- non devono essere basate su informazioni personali, come nomi di membri della famiglia, date di nascita, anagrammi o combinazione di nomi e simili
- un altro importante accorgimento riguarda la scelta di password che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo il tempo di digitazione ed evitare che la digitazione possa essere osservata surrettiziamente da terzi nelle vicinanze.

Ecco qualche indicazione per creare delle password sicure ma facili da ricordare:

- creare una password, basata sul titolo di una canzone o su un'altra frase, debitamente sintetizzata - ad esempio "*7000 caffè # Alex Britti*" diventa "7000cff#AB"
- la password può essere formata abbreviando un'intera frase, come ad esempio "Chi fa da sé fa per 3!" diventa "Cfdaséfx3!".

Attenzione: si raccomanda, per ovvi motivi, di non usare MAI come password proprio gli esempi sopra illustrati!

Password deboli

Si sottolinea ancora una volta che le password deboli, cioè di facile individuazione e, quindi, facilmente violabili, hanno le seguenti caratteristiche:

- la password si può trovare in un comune dizionario italiano, in inglese od altra lingua comune
- la password è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di personaggi di fantasia
- sono da ritenere insoddisfacenti anche password legate a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili
- è da scartare una qualsiasi delle password precedentemente indicata come debole, preceduta o seguita da una o più cifre (come ad esempio: Giovanni1989, oppure 2020Giovanni)

Istruzioni e raccomandazioni per la protezione della password e la diligente custodia dei dispositivi di autenticazione in possesso ed uso esclusivo

Non utilizzare la stessa password sia per sistemi di autenticazione interni sia per sistemi di autenticazione esterni alla rete informatica del **Titolare**, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività non legate all'attività lavorativa.

La password prescelta non deve essere condivisa né comunicata con alcun soggetto, ivi inclusi i superiori, a qualsiasi livello, o i tecnici di help desk del CRC.

Di seguito un elenco degli accorgimenti da adottare:

- non rivelate una password attraverso il telefono a chicchessia
- non scrivete la password su un qualsiasi documento e non nascondetelo in alcuna parte del vostro ufficio
- non archiviate la password in chiaro in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare e simile
- non scrivete una password in un messaggio di posta elettronica

- non rivelate la password al vostro superiore
- non parlate di password di fronte a terzi
- non date alcuna indicazione in merito al formato ed alla lunghezza della password che utilizzate
- non svelate la password su questionari o su formulari di sicurezza
- non rivelate la password ad un vostro collega di lavoro
- non utilizzare mai la caratteristica, offerta da parecchie applicazioni, di memorizzare la password direttamente nell'applicazione o nella memoria del browser.
- Non riutilizzare password già utilizzate in precedenza ed evitare la "somiglianza", cioè evitare di scegliere password formate da combinazioni di caratteri che possano far scoprire la nuova a partire da una di quelle precedenti (ad es. se avete già utilizzato una vecchia password tipo: 2019Giovanni#, evitate di utilizzare una nuova password tipo: 2020Marcella#, etc.)

Inoltre, gli Incaricati a cui sono stati consegnati dei dispositivi per l'autenticazione forte (ad es. token usb, smart card, ecc.) sono personalmente responsabili della custodia di tali dispositivi e devono informare repentinamente un proprio Dirigente superiore nel caso di perdita o furto.

Nel caso di operazioni sistemistiche che richiedano la vostra password (es: cambio del PC o installazione di programmi), l'**Amministratore di Sistema** la cambierà con una temporanea, dandovene comunicazione. Al primo utilizzo del PC, è obbligatorio che modifichiate in segreto e subito la password temporanea, digitando una vostra password forte conforme ai criteri sopra menzionati.

Se qualcuno insiste per conoscere la vostra password, dapprima fate riferimento a questo documento e successivamente informate immediatamente il **Responsabile ICT o il vostro Dirigente.**

Se avete anche solo il minimo sospetto che la vostra password sia stata in qualche modo compromessa o sia venuta a conoscenza di terzi, provvedete immediatamente alla sostituzione della password e riferite l'accaduto all'**Amministratore di Sistema** o al **Responsabile ICT** e, nel caso in cui avete il minimo sospetto di una perdita di dati, occorre informare tempestivamente il Responsabile ICT e il Titolare riguardo al "Data Breach" subìto.

Si faccia attenzione che, nell'ambito delle misure di controllo del livello di sicurezza del Sistema informativo, è possibile che l'**Amministratore di Sistema** effettui volontariamente dei tentativi di violazione della vostra password, per verificarne la robustezza; nel caso il tentativo abbia esito positivo, l'**Amministratore di Sistema** vi chiederà di sostituire immediatamente la vostra password con una segreta e più forte di quella violata.

Nel caso si abbia qualsiasi dubbio afferente alle modalità sicure di generazione, utilizzo e conservazione delle password, ci si deve rivolgere all'**Amministratore di Sistema** o al **Responsabile ICT** per ottenere opportuni chiarimenti ed istruzioni.

Accesso ai dati ad opera del Titolare, in caso di emergenza

Si informa che il **Titolare** è tenuto ad adottare idonee e preventive procedure che consentano l'accesso ai dati e ai sistemi, protetti dalla componente riservata delle credenziali (password) o da dispositivi in uso esclusivo ai dipendenti, in caso di prolungata assenza o impedimento degli stessi e in caso si renda necessario e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del Sistema.

Resta inteso che dal momento in cui, per l'accesso ai dati in caso di emergenza, il **Titolare** o il **Responsabile ICT** e/o l'**Amministratore di Sistema** procedano al reset della password in uso esclusivo all'utente, allo stesso non compete più alcuna ulteriore responsabilità, in merito a trattamenti non autorizzati od accessi non consentiti ai dati personali, di cui al suo profilo di autorizzazione.

Tale responsabilità verrà pienamente rimessa in essere non appena l'utente avrà avuto la possibilità di selezionare una propria nuova password segreta e forte.

Disattivazione delle credenziali di accesso

Qualora ci si trovasse nella impossibilità ad accedere al sistema con le credenziali assegnate, occorre rivolgersi al **Responsabile ICT** o all'**Amministratore di Sistema**.

Nel caso di perdita del diritto di accesso, come ad esempio per cessazione del rapporto lavorativo, le credenziali assegnate saranno disattivate.

I file di lavoro saranno trasferiti ad altro soggetto interno, su indicazione del rispettivo Dirigente o Responsabile di ufficio.

Sessioni di trattamento dati incustodite

Si raccomanda di non lasciare incustodito e accessibile il PC durante una sessione di trattamento di dati personali, in particolare qualora sia necessario allontanarsi temporaneamente dal posto di lavoro.

In tal caso si ricorda che è possibile effettuare un blocco "manuale" della schermata di accesso. Infatti, la pressione contemporanea dei tasti Ctrl + Alt + Canc sulla tastiera, attiva la finestra di "Protezione di Windows" dalla quale è possibile cliccare poi sul pulsante "Blocca computer" per bloccare la stazione di lavoro, senza la necessità di uscire dai programmi in uso. Una volta ritornati davanti alla propria postazione, per riprendere l'operatività è necessario seguire le istruzioni a video delle finestre di Windows, premendo nuovamente i tasti Ctrl + Alt + Canc sulla tastiera e digitando la propria password.

Per cautelarsi ulteriormente dalle eventualità di lasciare sessioni di trattamento di dati personali incustodite, è possibile impostare anche un blocco "automatico" ("screen saver con password") della propria postazione di lavoro, che blocca la schermata di accesso dopo un certo tempo di inattività e richiede poi l'inserimento della password in fase di ripristino della

videata di accesso. Per far ciò è necessario eseguire le operazioni specifiche per ogni sistema operativo; rivolgersi al Responsabile ICT per un supporto specifico.

Il blocco "automatico" con password è da considerarsi, comunque, una misura atta a ridurre, e non ad eliminare totalmente (a causa del suo fisiologico ritardo di attivazione) possibili rischi di trattamento dati da parte di persone non autorizzate. E' necessario, pertanto, prendere tutte le cautele affinché ciò non avvenga, ad esempio volontariamente mediante il blocco della stazione di lavoro nella modalità "manuale" sopra identificata.

Istruzioni e raccomandazioni per l'organizzazione dei dati su File System (spazi di memorizzazione esterni ai database)

Si ricorda che, in generale, tutti i dati/documenti sono salvati e conservati "strutturati" nei rispettivi database (collegati agli applicativi in uso al CRC) che possono essere "*on premise*" (cioè conservati nel datacenter fisico del CRC) oppure "*on cloud*" (cioè conservati nei datacenter internazionali dei fornitori di servizi cloud).

Per quanto riguarda dati e documenti da conservare sul file system (cioè direttamente sui dischi, ma fuori dai database), si ricorda che è vietato e NON sicuro conservare dati e documenti solo sui dischi della propria postazione (infatti, in caso di guasto fisico sul disco del PC, spesso tali dati e documenti non sono più recuperabili e sarebbero perduti per sempre). Pertanto, le uniche aree autorizzate al salvataggio di dati "non strutturati" su file system sono le cartelle "riservate" sui server del CRC (es. nell'area intranet) o sul cloud del CRC (es. su OneDrive® o su Sharepoint®), le quali sono configurate per consentire l'accesso solo agli aventi diritto (cioè solo a uno o più utenti autorizzati, ai quali sono stati abbinati i relativi privilegi di accesso a quella specifica cartella, ad es. solo lettura, oppure lettura/scrittura/modifica, etc.) .

Le cartelle possono essere caratterizzate come segue:

- Ogni utente autorizzato dispone di una propria cartella personale (ad es. <cognome.3inizialinome> resa accessibile solo a lui e, preterintenzionalmente, agli Amministratori di Sistema.
- Ogni Ufficio /Struttura dispone di una propria cartella condivisa (ad es. 1ComPerm, Seduta_consiliare, etc–resa accessibile solo al Dirigente /Responsabile di Uffiio/ Struttura ed agli utenti da questi autorizzati

Tali spazi sono configurati al fine di garantire la sicurezza e la custodia dei dati in conformità a quanto previsto dal profilo di incarico assegnato, impedendo accessi non consentiti, assicurando disponibilità dei dati in caso di emergenza e sottoposti a backup.

Qualora un utente, accedendo al server, si accorga di:

- aver involontariamente cancellato un file
- aver involontariamente corrotto un file
- non reperire il file che si vuole aprire

è necessario che si rivolga al **Responsabile ICT** o all'**Amministratore di Sistema**.

Nel caso non sia stato possibile il recupero dei file, il **Responsabile ICT** o l'**Amministratore di Sistema,** insieme all'incaricato, valuterà l'opportunità, in caso di sospetta perdita di dati personali, di comunicare l'avvenuto Data Breach.

Ogni salvataggio di dati e/o documenti sul PC locale è fortemente sconsigliato ed è sotto la esclusiva e totale responsabilità dell'incaricato.

Per chi dispone di notebook ed abbia necessità di avere sul disco locale dei documenti, è opportuno attivare una procedura di **sincronizzazione automatica dei file,** chiedendo autorizzazione al proprio Dirigente/ Responsabile di struttura e coinvolgendo il **Responsabile ICT** o l'**Amministratore di Sistema**.

Se invece si utilizzano supporti rimovibili (cd-rom, chiavette USB, etc…) per il trasferimento e la modifica di file, occorre mantenerne una copia aggiornata, sul server della rete informatica del **Titolare**.

Istruzioni e raccomandazioni per la custodia, uso e distruzione di supporti rimovibili

In linea generale, non è permessa la copia su supporti rimovibili (cd/dvd, chiavette USB, hard disk, ecc.) di dati personali, al fine di ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi.

Ciò premesso, ove nello svolgimento della normale attività assegnata, nell'ambito del profilo di autorizzazione, sia indispensabile effettuare una copia di dati personali su supporti rimovibili, occorre attenersi alle seguenti cautele:

- utilizzare solo ed esclusivamente supporti forniti dal Titolare e con l'autorizzazione del proprio Dirigente/Responsabile o del Responsabile ICT.
- accertarsi che il supporto rimovibile sia debitamente formattato e privo di altri file, che potrebbero essere infettati da virus a contenere dati di natura diversa; nel dubbio, è sempre bene provvedere alla formattazione *ex novo* del supporto, prima di registrarvi dati personali
- ove possibile, i dati devono essere protetti da un sistema di cifratura
- qualsiasi supporto rimovibile deve essere contrassegnato da un'etichetta, con una indicazione in chiaro od in codice, tale da permettere di riconoscere immediatamente il contenuto del supporto in questione, ed evitare che si possa confondere con altri supporti e facilitare la procedura di identificazione del supporto smarrito per l'eventuale segnalazione del Data Breach.

- I supporti rimovibili contenenti dati personali devono essere sempre direttamente e personalmente custoditi da chi ha realizzato la copia.

Qualora i dati contenuti su supporti rimovibili non abbiano più ragione di essere, si deve provvedere immediatamente alla formattazione dei supporti.

Poiché i supporti rimovibili potrebbero essere danneggiati da campi magnetici, per evitare la perdita anche accidentale dei dati, tali supporti non devono mai essere avvicinati ad un campo magnetico, come ad esempio il magnete di un altoparlante, oppure i trasformatori utilizzati nelle lampade da tavolo.

Si faccia sempre attenzione a non dimenticare il supporto rimovibile all'interno del computer, quando lo si spegne o ci si allontana.

Il supporto rimovibile contenente dati personali non deve mai essere lasciato incustodito, ma deve essere posto all'interno di una custodia sicura. In funzione della criticità dei dati archiviati e quindi del contenuto di eventuali dati sensibili, può essere considerato sicuro un cassetto della scrivania chiuso a chiave, oppure un armadio chiuso a chiave, una cassaforte chiusa, o un altro contenitore idoneo alla custodia di tali supporti e con opportuna serratura.

Se il supporto viene smarrito o rubato occorre immediatamente avviare la procedura di rilevazione del Data Breach.

Istruzioni e raccomandazioni per l'utilizzo di hardware e software

Il software installato in ciascuna macchina (Sistema operativo, Office Automation, etc.) nonché le relative configurazioni hardware, rispecchiano la condizione necessaria e sufficiente per il consueto lavoro da svolgersi e comunque valutato e stabilito dal **Titolare**.

Qualora si ritenga necessario disporre di un nuovo software o di un aggiornamento hardware per le consuete mansioni, è proibito procedere all'auto-installazione dei medesimi ma è necessario informare l'**Amministratore di Sistema** che valuterà l'opportunità dell'upgrade della macchina.

È bene ricordare che ogni software ha una licenza e l'uso improprio di questa può portare a conseguenze civili.

Inoltre, agli utenti dei Personal Computer del CRC non è consentito l'accesso ai parametri di configurazione dei software e del Sistema Operativo, per modificare i quali è sempre necessaria una specifica attività da parte degli Amministratori di Sistema.

Istruzioni e raccomandazioni per l'utilizzo di internet e del servizio e-mail

L'utilizzo di internet e della posta elettronica, sono resi disponibili dal **Titolare** per scopi lavorativi, cioè al fine di ottemperare alle mansioni previste dal proprio ruolo.

Per approfondimenti su tali tematiche, si veda il documento:

DPMS 02-001_Regolamento interno privacy per posta elettronica e internet

Istruzioni e raccomandazioni per la rilevazione e protezione dalle minacce di phishing

Il phishing è un'azione volta al furto dell'identità informatica, cioè di quelle informazioni, generalmente riservate, che permettono di identificare un soggetto che accede ad un sistema informatico (es. le credenziali di accesso al pc, le credenziali di accesso al portale internet del conto corrente bancario, ecc.).

Il phishing inizia con la ricezione di una e-mail, inviata dal truffatore alle potenziali vittime. Di norma, il messaggio di posta ha un aspetto formale e cerca di indurre il destinatario ad effettuare una serie di operazioni abbastanza usuali per coloro che usufruiscono dei servizi web on-line.

Un esempio: l'invito a "cliccare" sull'indirizzo del sito (in questo caso pirata) e la presentazione di una pagina web, artefatta ma molto verosimile, che appare con tutte le caratteristiche dell'azienda con la quale l'utente ha stipulato il servizio on-line. Se la vittima cade nella trappola e inserisce i propri dati tramite l'apposita pagina web, scatta il meccanismo di raccolta delle informazioni che, una volta in possesso del truffatore, possono essere usate in modo fraudolento.

Si riporta un esempio di e-mail "phishing".

"*Gentile Cliente,*

questa e-mail Le è stata inviata dai server di (di solito il nome di una banca) per evitare che il suo account (nome utente e password) sia disattivato per inutilizzo. Per completare l'operazione è sufficiente che Lei faccia click sul link seguente ed effettui il log-in come di consueto. Tutto questo per garantire la protezione dei suoi dati. Infatti è stato riscontrato che molti utenti non effettuano l'accesso da tanto tempo. Per verificare il suo account faccia click sul link seguente e, quindi, effettui il log-in come di consueto: www.nomebanca.com/verificaaccount "

Per scongiurare le minacce di phishing è utile attenersi ai seguenti punti:

- evitare di rispondere a richieste di informazioni personali ricevute tramite posta elettronica, se non si ha certezza della provenienza. Nel dubbio, è sempre preferibile verificare l'attendibilità dell'informazione o della richiesta contattando il mittente con canali diversi (es. telefono).
- anche se il link nella e-mail o la barra degli indirizzi web risulta (apparentemente) corretto, è bene sapere che esistono delle tecniche, usate dagli hacker, per mascherare l'indirizzo fasullo con uno corretto. Se c'è il minimo sospetto è meglio evitare di "cliccare" sui link per accedere ai relativi siti web. Questi collegamenti potrebbero condurre al sito pirata. Invece, aprire una nuova finestra del browser e digitare "a mano" l'indirizzo.
- i siti legittimi che richiedono informazioni riservate codificano (criptano) sempre la sessione. Quindi accertarsi sempre che il sito web che richiede i dati, adotti dei validi sistemi di crittografia, per esempio SSL - Secure Sockets Layer, verificando la presenza

dell'icona del "lucchetto" sulla parte in basso a destra del browser (fare doppio click sul lucchetto per verificare il certificato SSL).

In ogni caso, è opportuno notificare al **Responsabile ICT** o all'**Amministratore di Sistema** eventuali sospetti di phishing, furto d'identità o usi illeciti delle proprie informazioni e, nel caso ci fosse il fondato sospetto di una violazione dei dati personali, occorre informare il referente della procedura sul Data Breach.

Istruzioni e raccomandazioni per la rilevazione e protezione dalle minacce di pharming

Il pharming è un'estensione estremamente sofisticata del phishing. A differenza di quest'ultimo, gli attacchi di Pharming rimangono nascosti in un computer connesso alla rete e raccolgono informazioni sui dati finanziari durante la normale navigazione delle vittime. Gli utenti che vogliono collegarsi a un sito web sono, a loro insaputa, dirottati verso un sito artefatto, simile a quello originale. Una volta impiantato lo schema di pharming, può partire l'attività dannosa contro un gran numero di siti che l'utente visita regolarmente, senza che la vittima se ne renda minimamente conto.

Per identificare le minacce di pharming, è utile sapere che:

- i processi di login, verifica o informazione mostrati nei siti pirata non sono esattamente identici a quelli del sito autentico
- è probabile che i siti di pharming richiedano informazioni di verifica o personali che solitamente non sono necessarie
- i siti legittimi che richiedono informazioni riservate codificano (criptano) sempre la sessione. Quindi accertarsi sempre che il sito web che richiede i dati, adotti dei validi sistemi di crittografia, per esempio SSL - Secure Sockets Layer, verificando la presenza dell'icona del "lucchetto" sulla parte in basso a destra del browser (fare doppio click sul lucchetto per verificare il certificato SSL)
- in un sito sicuro, l'indirizzo (URL) che compare nel browser dovrebbe contenere il prefisso **https://** (che è **s**icuro) nella barra dell'indirizzo. I siti di pharming generalmente non hanno certificati SSL, per cui il prefisso **http://** (che è non sicuro) rimane anche quando si devono inserire dati riservati
- se il browser rileva l'esistenza di un problema con il certificato SSL, invece di ignorarlo, gli utenti devono cogliere l'occasione per controllare il certificato e considerarlo come un segno evidente di sito fraudolento.

In ogni caso, è opportuno notificare al **Responsabile ICT** o all'**Amministratore di Sistema** eventuali sospetti di pharming e, nel caso ci fosse il fondato sospetto di una violazione dei dati personali, occorre informare il referente della procedura sul Data Breach.

Istruzioni per il trattamento di dati senza l'ausilio di strumenti elettronici

Gestione quotidiana pratiche

Istruzioni per i dati personali in genere

- Le pratiche contenenti dati personali (di seguito: "le pratiche") devono essere di norma riposte in archivi chiusi. Si considera archivio chiuso anche il locale chiuso a chiave
- Le pratiche devono essere prelevate, a cura degli utilizzatori, solo nella misura e per il tempo strettamente necessari per lo svolgimento dei relativi compiti, al termine dei quali – ed in ogni caso al termine della giornata lavorativa – devono essere riposte negli archivi. Ciascun utilizzatore deve aver cura di verificare che le pratiche affidategli non restino incustodite, specie in contesti accessibili a soggetti non incaricati del trattamento (aree di passaggio, sale d'attesa, ecc.).
- Anche durante la giornata lavorativa, in caso di allontanamento dalla postazione di lavoro per un periodo di tempo significativo, le pratiche devono essere riposte negli archivi, salvo adeguata garanzia di controllo da parte di altri utilizzatori autorizzati ai medesimi trattamenti. In ogni caso le pratiche non devono essere mai lasciate incustodite.
- Lo smarrimento o il furto di informazioni devono essere comunicati immediatamente al referente della procedura sul Data Breach.
- È buona regola evitare la proliferazione eccessiva di stampe e fotocopie di documenti contenenti dati personali. Le stampe e le fotocopie inutili devono essere distrutte nell'apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi piccoli.

Istruzioni per le categorie particolari di dati e per i dati relativi a condanne penali o reati

Oltre a quanto previsto per i dati personali in genere, le pratiche contenenti categorie particolari di dati, e dati relativi a condanne penali o reati, devono essere conservate in archivi ad accesso controllato, devono essere controllate e custodite dagli incaricati fino alla restituzione, in maniera che ad essi non accedano persone prive di autorizzazione (ivi compresi altri utilizzatori che non siano autorizzati ad accedere alle informazioni sensibili) e devono poi essere restituite al termine delle operazioni affidate.

Compete agli utilizzatori il controllo della chiusura a chiave degli armadi contenenti tale tipologia di dati e la chiusura dei propri uffici in caso di temporaneo allontanamento ed alla fine dell'orario lavorativo.

Gestione chiavi

I soggetti chiamati a gestire le chiavi "fisiche" degli archivi devono:

- all'atto della consegna delle chiavi, verificarne subito il corretto funzionamento;
- verificare che le chiavi non restino inserite negli armadi/archivi;
- conservare le chiavi in un luogo e con modalità che ne garantiscano una sicurezza adeguata anche al tipo di archivio;
- non metterle a disposizione né mostrarle ad estranei;
- in caso di smarrimento o sottrazione, farne immediata segnalazione al referente della procedura sul Data Breach e richiedere la sollecita sostituzione della serratura, spostando se del caso, per il tempo necessario, i documenti dall'archivio non protetto ad altro luogo sicuro.

Compete a tali soggetti il controllo della chiusura a chiave degli armadi contenenti dati sensibili e la chiusura dei propri uffici in caso di temporaneo allontanamento ed alla fine dell'orario lavorativo.

Scarti di archivio

Gli scarti di archivio, ossia il periodico smaltimento di materiale cartaceo contenente dati personali, deve essere effettuato evitando che le informazioni personali, specie se sensibili, possano essere trattate da soggetti non incaricati/autorizzati.

In particolare, i documenti contenenti categorie particolari si dati devono essere smaltiti mediante utilizzo degli appositi strumenti per la distruzione, ove disponibili, altrimenti vanno ridotti in piccoli pezzi.

Consegna di certificazioni medico-sanitarie a mezzo di altri soggetti

La consegna di certificazioni mediche, o comunque di altre informazioni personali delicate relative ai dipendenti o a terzi, può essere effettuata anche tramite altri dipendenti o comunque altre persone a condizione che:

- la documentazione sia di regola consegnata in busta chiusa;
- prima della consegna, la documentazione non sia lasciata incustodita; di regola, ove non sia presente il destinatario, la documentazione va consegnata a un Dirigente/ Responsabile di struttura;
- la consegna avvenga nel minor tempo possibile.

Uso di scanner digitali e telefono ufficio

Riguardo alle multifunzioni (fotocopiatrici digitali con scanner di rete), il loro utilizzo è consentito per l'invio delle scansioni tramite e-mail o, se previsto nelle specifiche sedi, via rete o FTP ad una cartella di rete accessibile a tutti gli incaricati.

È necessario adottare le seguenti cautele:

- le scansioni contenenti categorie particolari di dati personali devono avvenire esclusivamente via e-mail.
- le scansioni inviate via FTP devono essere cancellate immediatamente dopo la scansione ed il successivo salvataggio da parte dell'incaricato che le ha effettuate.
- in ogni caso è prevista la cancellazione automatica di tali aree ogni venerdì sera.

Telefonate e colloqui

Informazioni telefoniche

Il personale deve considerare che il colloquio telefonico non è, di norma, metodo adeguato per l'identificazione sicura dell'interlocutore.

Deve essere pertanto rispettata la seguente regola generale: non è consentito fornire informazioni personali telefonicamente, in quanto non è di norma possibile identificare con certezza la persona con la quale è in corso il colloquio.

La regola generale può trovare eccezioni tutte le volte in cui si possa ragionevolmente ritenere di avere sufficienti elementi per l'identificazione certa dell'interlocutore (ad esempio, in quanto esiste con l'interlocutore una consuetudine di rapporto, tale da garantire di fatto il riconoscimento; oppure in forza di una verifica su alcuni dati personali – data di nascita, codice fiscale, ecc.; e così via).

Comportamento nel corso delle telefonate

Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, anche utilizzando cellulari, per evitare che dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente.

Misure di controllo e verifica

Al fine di forzare, monitorare e verificare l'adozione delle misure di sicurezza, il **Titolare**, relativamente agli strumenti elettronici di trattamento dati, adotta i seguenti accorgimenti tecnici:

- ai nuovi utenti sarà obbligatoriamente richiesta la scelta di una password personale al primo accesso al sistema
- non saranno accettate dal sistema password di lunghezza inferiore a 10 caratteri
- saranno accettate dal sistema solo password contenenti caratteri di almeno tre delle seguenti categorie:
    - lettere maiuscole (da A a Z)
    - lettere minuscole (da a a z)
    - numeri (da 0 a 9)
    - caratteri non alfanumerici (ad esempio,!, $, #, %)
- il sistema ricorderà agli utenti l'avvicinarsi della scadenza della propria password e imporrà il cambio della stessa allo scadere, impostato almeno ogni 3 mesi per gli account autorizzati al trattamento di dati sensibili, ogni 6 mesi per gli altri.
- Ove possibile il sistema verificherà che la nuova password inserita sia differente dalle ultime 6 utilizzate.

Inoltre, il **Titolare** effettuerà, periodicamente, specifiche verifiche al fine di valutare se gli strumenti elettronici affidati sono usati in attinenza all'ambito lavorativo e secondo le istruzioni impartite.

Relativamente al trattamento di dati senza l'ausilio di strumenti elettronici, il **Titolare** effettuerà, periodicamente, specifiche verifiche al fine di valutare se sono seguite le procedure e le istruzioni impartite.

Istruzioni da seguire in caso di Data Breach

Nel caso in cui vi sia il fondato sospetto che si sia verificata una violazione di dati, come ad esempio:

- Perdita di documenti o fascicoli
- Distruzione archivi
- Furto o smarrimento di strumenti elettronici contenenti dati personali
- Sospetto di accesso non autorizzato nei locali deputati all'archiviazione
- Sospetto di accesso non autorizzato nel Datacenter
- Sospetto di accesso non autorizzato nel proprio PC
- Comportamento anomalo del proprio PC o dispositivo informatico

- etc.…

Occorre informare tempestivamente il referente della procedura sul Data Breach, comunicandogli il maggior numero di dettagli circa la violazione subita:

- Data in cui è avvenuto l'evento o in cui si è venuti a conoscenza dello stesso
- Modalità di esposizione al rischio, ad es.:
  - Lettura dei dati personali
  - Copia dei dati personali
  - Alterazioni dei dati personali
  - Cancellazione dei dati personali
  - Furto dei dati personali
- Dati personali oggetto della violazione (dati dei dipendenti, dei clienti, etc.)

Sanzioni

Il personale dipendente che abbia violato le linee guida di sicurezza riportate nel presente documento potrebbe essere sottoposto ad azioni disciplinari, per i possibili riflessi che la sua negligenza potrebbe avere avuto sulla sicurezza relativa alla protezione dei dati personali.

Consiglio Regionale della Campania

Procedura e modello per la nomina dei Responsabili

GESTIONE DELLE MODIFICHE

Versione	Data emissione	Descrizione delle modifiche
1.0	25 MAGGIO 2020	Prima emissione

Indice dei contenuti

1 INTRODUZIONE

Il presente documento descrive i principi generali che disciplinano la nomina dei Responsabili esterni del trattamento nei rapporti contrattuali con i soggetti terzi ai quali sono affidate attività che comportino un trattamento di dati personali.

Ai fini del Regolamento UE 2016/679 si intende per Responsabile esterno del trattamento una persona fisica o giuridica, un'autorità pubblica, un servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento (art. 4, comma 8).

La nomina del Responsabile esterno del trattamento da parte del Titolare in alcuni casi è obbligatoria. Se designato, il Responsabile è individuato tra i soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del Regolamento 2016/679 e garantire la tutela dei diritti dell'interessato (art. 28, comma 1).

DESTINATARI

Il presente documento si applica al Consiglio regionale della Campania ("CRC") e a tutti gli uffici preposti all'affidamento di servizi all'esterno mediante bandi di gara e appalti (sopra e sottosoglia).

NORMATIVA DI RIFERIMENTO

Regolamento UE 2016/679 - Regolamento generale sulla protezione dei dati (o GDPR, General Data Protection Regulation).

PRINCIPI GENERALI

La designazione di un Responsabile esterno del trattamento (o di un sub-responsabile) deve garantire che vengano rispettate tutte le prescrizioni del Regolamento UE 2016/679.

CRC, pertanto, in qualità di Titolare del trattamento, deve ricorrere unicamente a Responsabili esterni del trattamento che presentino garanzie in termini di conoscenza specialistica, affidabilità e risorse per gestire la sicurezza dei dati, e che garantiscano l'applicazione di tutte le misure tecniche e organizzative previste dal Regolamento UE 2016/679.

NOMINA DEL RESPONSABILE DEL TRATTAMENTO

CRC, in qualità di Titolare del trattamento, deve provvedere alla nomina del Responsabile esterno del trattamento in tutti i casi in cui una terza parte - in qualità di fornitore, partner commerciale, appaltatore, subfornitore, subappaltatore, etc. - esegue per conto di CRC, attività, servizi o forniture che comportino un trattamento di dati personali, e tale soggetto non può essere considerato come autonomo titolare o un contitolare del relativo trattamento.

La nomina a Responsabile deve essere formalizzata dal CRC con apposita lettera o atto scritto a firma dei soggetti autorizzati ad agire in nome e per conto del Titolare.

Il Responsabile esterno del trattamento designato formalmente dal CRC si obbliga a rispettare la normativa in materia di Protezione dei Dati Personali e a trattare tali dati secondo le istruzioni impartite dal Titolare. È facoltà del CRC concedere al Responsabile un margine di discrezionalità in merito alla scelta dei mezzi tecnici ed organizzativi più adatti per l'esecuzione delle attività affidate. Tale margine non può riguardare comunque aspetti essenziali relativi al trattamento previsti dal Regolamento UE 2016/679 (attinenti ad esempio alle modalità e alle finalità con cui sono trattati i dati, alla durata della conservazione, all'accesso ai dati ed ad altre misure di sicurezza implementate).

Il Responsabile esterno del trattamento si impegna inoltre a cooperare con il CRC in qualsiasi momento al fine di assicurare il corretto trattamento dei dati personali e si impegna a fornire al CRC tutte le informazioni o i documenti che potranno essere richiesti da quest'ultima per l'adempimento degli obblighi di legge e per comprovare l'adozione delle misure tecniche e organizzative definite in qualità di Titolare.

CONTRATTO DI DESIGNAZIONE

L'esecuzione di un trattamento da parte di un Responsabile deve essere disciplinata da un contratto o da un altro atto giuridico a norma di legge, che vincoli il Responsabile esterno del trattamento al CRC ed al rispetto delle istruzioni impartite.

Tale contratto deve indicare chiaramente la natura e le finalità del trattamento, il tipo di dati personali, le categorie di interessati, la durata del trattamento e i compiti e le responsabilità specifici del Responsabile esterno del trattamento nel contesto del trattamento da eseguire (art. 28, comma 3).

Tale contratto deve prevedere, in particolare, che il Responsabile esterno del trattamento:

- tratti i dati personali soltanto su istruzione documentata del CRC quale Titolare del trattamento;
- garantisca che il personale autorizzato al trattamento dei dati personali si sia impegnato alla riservatezza o abbia un adeguato obbligo legale di riservatezza;
- adotti tutte le misure tecniche ed organizzative sulla sicurezza dei dati richieste ai sensi dell'articolo 32 del Regolamento UE 2016/679;
- assista il CRC, in qualità di Titolare, con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
- tenendo conto della natura del trattamento e delle informazioni a sua disposizione, assista il CRC, in qualità di Titolare, nel garantire il rispetto degli obblighi previsti dagli articoli da 32 a 36 del Regolamento (sicurezza del trattamento, notifica di una violazione dei dati personali al Garante Privacy, comunicazione di una violazione dei dati personali all'interessato, valutazione d'impatto sulla protezione dei dati, consultazione preventiva);
- al termine della prestazione dei servizi relativi alle attività di trattamento, cancelli o restituisca al CRC, in qualità di Titolare, tutti i dati personali trattati, cancellando anche eventuali copie di dati esistenti (salvo che la legislazione cui è soggetto il Responsabile ne prescriva la conservazione);
- metta a disposizione del CRC, in qualità di Titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dal Regolamento UE 2016/679;
- contribuisca alle attività di revisione eseguite dal CRC in qualità di Titolare del trattamento, comprese le ispezioni, o da un altro soggetto incaricato dal CRC.

In caso di accordi o contratti con fornitori o appaltatori, la nomina a Responsabile esterno del trattamento si intende tacitamente rinnovata ad ogni rinnovo dell'accordo o contratto. Si intende tacitamente revocata alla scadenza dell'accordo/contratto stesso o in qualsiasi caso di cessazione anticipata, salva la revoca anticipata per qualsiasi motivo da parte del CRC. Al fine di uniformare le modalità di conferimento di tali accordi/nomine a responsabili esterni del trattamento, il personale del CRC è tenuto a prendere come riferimento i modelli allegati alla presente procedura (Mod. 06-002 – Mod. 06-003).

OBBLIGHI DEL TITOLARE

Il Regolamento UE 2016/679 prevede che le misure che il Titolare deve adottare siano sempre basate sulla valutazione del rischio derivante da una specifica attività trattamento.

Tale valutazione deve tenere conto soprattutto dal trattamento svolto da parte di soggetti esterni. Il contratto stipulato tra il CRC e il Responsabile esterno del trattamento deve includere, pertanto, tutte le misure che questo deve adottare per garantire che il trattamento a lui affidato non determini una variazione della valutazione di rischio rispetto a quella definita dal CRC.

Il Regolamento UE 2016/679 prevede che il Responsabile esterno del trattamento è tenuto a concorrere col Titolare, e ad assisterlo, per quanto riguarda le segnalazioni dei data breach.

Il contratto stipulato tra il CRC e il Responsabile esterno del trattamento deve, pertanto, porre obblighi chiari al Responsabile per la parte di sua competenza e prevedere un dovere specifico di segnalazione, tempestivamente e senza ingiustificato ritardo, di essere venuto a conoscenza di una violazione (distruzione, perdita, modifica, divulgazione non autorizzata dei dati personali), fornendo tutti i dettagli degli eventi occorsi nell'ambito dei trattamenti a lui affidati.

Il contratto stipulato tra il CRC e il Responsabile deve contenere inoltre obblighi per il Responsabile per assistere e supportare il CRC, in qualità di Titolare, per soddisfare l'obbligo di dare riscontro alle richieste per l'esercizio dei diritti degli interessati.

Ai sensi dell'art. 30 del Regolamento UE 2016/679 il CRC, in qualità di Titolare del trattamento, deve mantenere nel Registro delle attività di Trattamento l'elenco di tutti i Responsabili nominati per ciascun trattamento, con la rispettiva denominazione/ragione sociale.

OBBLIGHI DEL RESPONSABILE

Il Responsabile, nell'adempimento dei propri doveri, ha obblighi di trasparenza nei confronti del Titolare. Il Responsabile, ricevuto l'atto giuridico con tutte le istruzioni in merito ai trattamenti che deve operare per conto del CRC, si deve impegnare, pertanto, ad effettuare il Trattamento dei soli Dati Personali necessari e/o strumentali all'esecuzione del contratto.

Il Responsabile esterno del trattamento, nell'adempimento dei propri doveri, ha obblighi di garantire la sicurezza dei dati. Si deve impegnare a livello contrattuale, pertanto, ad adottare le misure tecniche ed organizzative previste dall'art.32 del Regolamento UE 2016/679, tra le quali anche le misure di attuazione dei principi di privacy by design e by default, e assicura che le misure di sicurezza progettate ed implementate siano in grado di garantire la riservatezza dei dati e ridurre il rischio di danni volontari o accidentali, perdita di dati, accessi non autorizzati ai dati, trattamenti non autorizzati o trattamenti non conformi alle finalità indicate dal CRC.

Il Responsabile esterno del trattamento si deve impegnare anche ad assistere il CRC nel garantire il rispetto degli obblighi relativi alla sicurezza del trattamento, alla valutazione d'impatto sulla protezione dei dati, alla notifica di una violazione dei dati personali all'Autorità di controllo e alla comunicazione di una violazione dei dati personali all'interessato.

In particolare, in caso di violazione dei dati personali subita dal Responsabile e che ne determini la distruzione, perdita, modifica o divulgazione non autorizzata, il Responsabile deve informare il CRC, tempestivamente e senza ingiustificato ritardo, di essere venuto a conoscenza di una violazione e fornire tutti i dettagli completi della violazione subita (descrizione, volume dei dati personali interessati, natura della violazione, i rischi per gli interessati e le misure adottate per mitigare i rischi).

Il Responsabile esterno del trattamento si deve impegnare anche a mantenere in un apposito Registro delle attività di Trattamento ai sensi dell'art. 30 del Regolamento UE 2016/679 l'elenco di tutti i trattamenti per i quali è stato nominato dal CRC Responsabile.

Il Responsabile esterno del trattamento si deve impegnare, altresì, ad assistere e supportare il CRC per dare riscontro alle richieste per l'esercizio dei diritti degli interessati. Qualora il Responsabile riceva richieste provenienti dagli Interessati finalizzate all'esercizio dei propri diritti, dovrà darne tempestiva comunicazione scritta al CRC e coordinarsi, per quanto di propria competenza, per gestire le relazioni con gli Interessati.

Il Responsabile esterno del trattamento può ricorrere ad un altro Responsabile solo se è stato preventivamente autorizzato dal CRC tramite il contratto sottoscritto.

In caso di autorizzazione, il Responsabile esterno del trattamento deve informare il CRC di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri Responsabili del trattamento. Il CRC, in qualità di Titolare, deve valutare le garanzie offerte dal nuovo Responsabile proposto, opponendosi se non le ritiene adeguate.

In caso di autorizzazione a ricorrere ad altro Responsabile per l'esecuzione di specifiche attività di trattamento, il Responsabile principale dovrà applicare al nuovo Responsabile gli stessi obblighi in materia di protezione dei dati previsti dal contratto con il CRC. Nel caso in cui il nuovo Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile principale conserva nei confronti del CRC l'intera responsabilità dell'adempimento degli obblighi previsti dal Regolamento UE 2016/679.

Il Titolare del Trattamento

Consiglio regionale della Campania

ACCORDO PER LA PROTEZIONE DEI DATI PERSONALI E
DESIGNAZIONE QUALE RESPONSABILE ESTERNO DEL TRATTAMENTO
(ART. 28 REG. UE 2016/679)

Il Consiglio regionale della Campania, con sede in Napoli Centro Direzionale, Isola F13 – 80143, Codice Fiscale e P. IVA 80051460634 (di seguito la "**CRC**" o il "**Titolare**"), in qualità di Titolare del trattamento ai sensi del Regolamento UE 2016/679 (di seguito "**GDPR**"), in persona del Presidente, dr.ssa Rosa D'Amelio.

E

_____*inserire nome ditta*_____**, con sede legale _____, in persona del legale rappresentante pro tempore (di seguito "**Fornitore**" o "**Responsabile**")

Congiuntamente indicate come le "**Parti**".

Premesso che

- il CRC ed il Fornitore hanno sottoscritto un contratto avente ad oggetto _____ e che comporta l'elaborazione dei dati di cui CRC è Titolare" (di seguito il **"Contratto**"), ed ai fini dell'esecuzione di detto Contratto il Fornitore dovrà effettuare operazioni di trattamento dei Dati Personali per conto di CRC;
- il perfezionamento del Contratto di cui al punto precedente comporta la necessità di trattare, in nome e per conto del suddetto Titolare, dati personali che come tali sono soggetti all'applicazione della Normativa in materia di Protezione dei Dati Personali;
- CRC svolge il ruolo di Titolare del trattamento in relazione ai Dati Personali oggetto di trattamento, stabilendo autonomamente le finalità, le modalità ed i mezzi del trattamento;
- Il Fornitore è in possesso di adeguate competenze tecniche e *know-how* circa gli scopi e le modalità di trattamento dei Dati Personali, delle misure di sicurezza da adottare al fine di garantire la riservatezza, la completezza e l'integrità dei Dati Personali trattati, nonché circa le norme che disciplinano la protezione dei Dati Personali;
- CRC, in qualità di Titolare del trattamento, intende nominare il Fornitore, come previsto dal presente accordo sulla protezione dei dati personali, quale Responsabile del trattamento ed il Fornitore intende accettare tale nomina;
- con riferimento alla summenzionata nomina, con la sottoscrizione del presente documento le Parti intendono regolare i reciproci rapporti in relazione al trattamento dei Dati Personali effettuato dal Fornitore per conto del CRC.

Tutto ciò premesso, alla luce di quanto precede, le Parti stipulano quanto segue:

Definizioni

Fatta eccezione per i termini e le espressioni altrimenti definiti nel Contratto oggetto del servizio, i termini e le espressioni contrassegnate da iniziali maiuscole avranno il significato di seguito specificato:

Regolamento UE 2016/679	indica la norma europea di riferimento che disciplina la protezione dei Dati Personali ed è direttamente applicabile in ciascuno degli Stati Membri dell'Unione Europea.

"**Codice Privacy**"	indica la norma italiana che disciplina la protezione dei Dati Personali, ed in particolare il Decreto Legislativo 196/2003 e successive modifiche e integrazioni;
"**Contratto**"	indica l'accordo sottoscritto tra le Parti per il tramite del quale avviene il trattamento dei dati per conto del Titolare;
"**Dato/i Personale/i**"	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»), così come definito all'articolo 4, comma 1, del Regolamento UE 2016/679;
"Categorie Particolari di Dati"	indica ogni Dato Personale di natura "sensibile", così come indicato all'articolo 9, comma 1, del Regolamento UE 2016/679;
"**Dati Giudiziari**"	indica ogni Dato Personale relativo a condanne penali e ai reati o a connesse misure di sicurezza ovvero relativo a provvedimenti giudiziari, sanzioni penali, o carichi pendenti, o la qualità dell'imputato o indagato;
"**Responsabile**"	indica la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che tratta dati per conto del Titolare del trattamento dei Dati Personali;
"**Incaricato**"	le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile e che agiscono sotto l'autorità del Titolare o del Responsabile;
"**Interessato**"	la persona fisica identificata o identificabile a cui si riferiscono i Dati Personali;
"**Autorità**"	indica il Garante per la protezione dei Dati Personali;
"**Collaboratore/i esterno/i**"	indica qualunque persona fisica o giuridica che nello svolgimento della propria attività professionale o commerciale nei confronti del Fornitore, effettui il trattamento dei Dati Personali di titolarità del CRC;
Sub-Responsabile/i	indica un altro responsabile (sub-Fornitore) del trattamento (persona fisica o giuridica) incaricato dal Fornitore ad effettuare il trattamento dei Dati Personali di titolarità del CRC;
"**Terze Parti o Terzi**"	indica quei soggetti estranei all'organizzazione delle Parti.

1. **Nomina del Responsabile del trattamento**

Con la sottoscrizione del presente documento, il CRC designa il Fornitore quale Responsabile del Trattamento, con l'incarico di effettuare le operazioni di trattamento sui Dati Personali di cui entra in possesso o a cui ha comunque accesso, necessarie all'adempimento degli obblighi derivanti dal Contratto e di eventuali servizi accessori allo stesso.

Il Fornitore, nonché i suoi dipendenti ed ogni Collaboratore esterno di cui il Fornitore si avvalga (per finalità strumentali all'oggetto principale del Contratto) e che effettui operazioni di trattamento su Dati Personali di titolarità del CRC, si obbliga a rispettare la Normativa in materia di Protezione dei Dati Personali ed ogni altra istruzione impartita dal CRC, tenendo conto dei provvedimenti tempo per tempo emanati dall'Autorità Garante per la protezione dei dati personali italiana ovvero dal Gruppo di Lavoro Articolo 29/Comitato Europeo per la protezione dei dati, inerenti al trattamento svolto.

Il Fornitore si impegna a cooperare con CRC in qualsiasi momento al fine di assicurare il corretto trattamento dei Dati Personali trattati e si impegna a fornire al CRC tutte le informazioni o i documenti che potranno essere ragionevolmente richiesti da quest'ultima per l'adempimento degli obblighi di legge e per comprovare l'adozione delle misure tecniche e organizzative adeguate da parte del CRC.

Il Fornitore, con la sottoscrizione del presente accordo, accetta tutti i termini sottoindicati, conferma la diretta e approfondita conoscenza degli obblighi che si assume in relazione al dettato normativo vigente e si impegna a procedere al trattamento dei Dati Personali attenendosi alle istruzioni ricevute dal Titolare attraverso la presente nomina o a quelle ulteriori che saranno conferite nel corso delle attività prestate in suo favore.

Il Fornitore prende atto che l'incarico è affidato per l'esclusiva ragione che il profilo professionale/societario, in termini di proprietà, risorse umane, organizzative ed attrezzature, è stato ritenuto idoneo a soddisfare i requisiti di esperienza, capacità, affidabilità previsti dalla vigente normativa. Qualsiasi mutamento di tali requisiti che possa sollevare incertezze sul loro mantenimento dovrà essere preventivamente segnalato al Titolare, che potrà esercitare in piena autonomia e libertà di valutazione il diritto di recesso, senza penali ed eccezioni di sorta.

2. **Natura e Finalità del trattamento**

Il trattamento deve essere svolto da parte del Responsabile in esecuzione dei vigenti rapporti contrattuali con CRC e per le relative finalità istituzionali, nonché per il tempo strettamente necessario al perseguimento di tali finalità. In particolare, i dati saranno trattati dal Responsabile, *mediante l'utilizzo di proprie infrastrutture hardware e software, per tutte le attività inerenti la _____[specificare la materia disciplinata dal contratto e le finalità perseguite dal CRC.*

3. **Tipologia di dati personali e Categorie di interessati**

Il trattamento dei dati personali, in riferimento ai Servizi affidati, riguarda dati di natura c.d. "comune" quali anagrafiche (*dati personali identificativi, codice fiscale e/o documenti di identità, coordinate di contatto, foto, immagini, etc.*) e/o relativi alla situazione economica, compreso eventuali "categorie particolari di dati" (relativi allo stato di salute, sindacali, etc.) e/o dati giudiziari[U1], in riferimento alle seguenti categorie di interessati: Consiglieri – Utenti –Cittadini Ue ed extra UE – Dipendenti – Minori – Anziani – Disabili - Fornitori – Professionisti – Dipendenti dei fornitori - Amministratori[U2].

4. **Obblighi e Diritti del Titolare**

CRC ha diritto di ottenere dal Responsabile tutte le informazioni relative alle misure organizzative e di sicurezza da questo adottate necessarie per dimostrare il rispetto delle istruzioni e degli obblighi affidati.

CRC, inoltre, ha il diritto di disporre - a propria cura e spese - verifiche a campione o specifiche attività di audit in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile, come indicato al punto 10.

CRC ha il diritto di conoscere l'esistenza di eventuali sub-responsabili al fine di rilasciare al Fornitore specifica autorizzazione. Il Fornitore, pertanto, accetta di comunicare tale elenco dietro semplice richiesta scritta da parte del CRC e si impegna a mantenere aggiornato detto elenco.

5. Obblighi del Responsabile

Il Responsabile, nell'adempimento delle proprie obbligazioni, si impegna ad effettuare il Trattamento dei soli Dati Personali che siano necessari e/o strumentali all'esecuzione del Contratto in essere. Il Responsabile si impegna, sin dalla data di sottoscrizione del presente documento, a rendere disponibili ed a comunicare ai propri Collaboratori esterni soltanto quei Dati Personali che siano strettamente necessari per l'adempimento delle obbligazioni di cui al Contratto in essere o che siano necessarie per l'adempimento di obblighi di legge o imposte dalle normative europee.

Il Responsabile si obbliga, nei limiti dei propri poteri, al rispetto delle norme che disciplinano il Trattamento dei Dati Personali, ivi incluse le regole stabilite dall'Autorità, ed a garantire che i propri dipendenti, ed ogni soggetto della cui cooperazione esso si avvalga, rispettino tali norme.

In particolare, il Responsabile si impegna a rispettare i seguenti obblighi e istruzioni:

5.1. Misure tecniche ed organizzative adeguate e violazioni dei dati personali

Il Responsabile dovrà adottare le misure tecniche ed organizzative adeguate previste dalla normativa italiana ed europea in materia di protezione dei Dati Personali, cosi come ogni altra previsione derivante dall'Autorità ovvero dal Gruppo di Lavoro Articolo 29/Comitato Europeo per la protezione dei dati.

Il Responsabile, in considerazione della conoscenza maturata quale conseguenza dei progressi tecnici e tecnologici, della natura dei Dati Personali e delle caratteristiche delle operazioni di Trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, si obbliga a mettere in atto misure tecniche ed organizzative adeguate e dovrà assicurare che le misure di sicurezza progettate ed implementate siano in grado di ridurre il rischio di danni volontari o accidentali, perdita di dati, accessi non autorizzati ai dati, trattamenti non autorizzati o trattamenti non conformi agli scopi di cui al presente Contratto.

In particolare, il Responsabile, anche per le attività di trattamento effettuate da ciascun dipendente e/o Collaboratore Esterno e ogni eventuale sub-fornitore (sub-responsabile) di cui si avvalga, si obbliga a:

5.1.1 adottare tutte le misure di cui all'art. 32 del Regolamento UE 2016/679 in modo da garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati, tenendo conto dei provvedimenti tempo per tempo emanati dall'Autorità Garante per la protezione dei dati personali italiana inerenti ai trattamenti svolti dal Responsabile;

5.1.2 consentire l'accesso ai propri sistemi informatici tramite l'utilizzo di identificativi univoci per ciascun utente, evitando identificativi condivisi tra più utenti, e attribuire a ciascun profilo di utenza i soli permessi di accesso ai sistemi necessari allo svolgimento delle rispettive mansioni operative (i permessi di accesso ai

sistemi sui quali sono archiviati dati di titolarità del CRC devono essere rivisti su base annuale e comunque revocati qualora questi non siano più necessari);

5.1.3 non trasferire i Dati Personali del CRC al di fuori dell'usuale luogo di lavoro, a meno che tale trasferimento non sia autorizzato dalle competenti pubbliche autorità, anche regolamentari e di vigilanza;

5.1.4 fornire al CRC, su specifica richiesta di quest'ultima, una descrizione dettagliata delle misure fisiche, tecniche ed organizzative applicate al Trattamento dei Dati Personali;

5.1.5 assistere CRC, relativamente ai dati oggetto di trattamento, nel garantire – ove applicabili – il rispetto degli obblighi relativi:

- alla sicurezza del trattamento;

- alla notifica di una violazione dei dati personali all'Autorità di controllo;

- alla comunicazione di una violazione dei dati personali all'interessato;

- alla valutazione d'impatto sulla protezione dei dati;

- alla consultazione preventiva.

In particolare, in caso di violazione dei dati personali subita dal Responsabile e che ne determini la distruzione, perdita, modifica, divulgazione non autorizzata dei dati personali, lo stesso Responsabile deve:

- informare CRC, tempestivamente e senza ingiustificato ritardo, e comunque nei termini di legge, di essere venuto a conoscenza di una violazione e fornire tutti i dettagli completi della violazione subita (descrizione, volume dei dati personali interessati, natura della violazione, i rischi per gli interessati e le misure adottate per mitigare i rischi);
- fornire assistenza al CRC per far fronte alla violazione e alle sue conseguenze (soprattutto in capo agli interessati coinvolti).

Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito.

Qualora venga rilevato che un'istruzione impartita dal Titolare vìoli le disposizioni relative alla normativa rilevante in tema di protezione dei dati personali, il Responsabile si obbliga ad informare immediatamente lo stesso Titolare di tale circostanza.

5.2. Modulistica Privacy

Il Responsabile dovrà adottare senza indugio la documentazione in materia di protezione dei dati personali prevista dalla normativa italiana ed europea in materia di protezione dei dati personali (tra cui il Registro delle Attività di trattamento ai sensi dell'art. 30 del Regolamento UE 2016/679) e le relative procedure concernenti le misure organizzative e di sicurezza.

Il Responsabile si impegna a fornire al Titolare una dichiarazione avente ad oggetto le misure tecniche ed organizzative relative al Trattamento adottate nell'ambito dell'esecuzione del presente Contratto e a fornire tempestivamente ulteriori chiarimenti al Titolare qualora da questi richiesti. In particolare, il Responsabile si impegna a fornire sin d'ora al Titolare la seguente documentazione:

- Registro dei Trattamenti del Responsabile (relativo ai Trattamenti effettuati per conto del Titolare nello svolgimento dei servizi);

- Elenco dei Sub-responsabili utilizzati per i trattamenti di dati effettuati per conto del Titolare (come indicato al punto 6);

- Elenco delle misure di sicurezza tecniche e organizzative adottate dal Responsabile;

- Elenco delle misure di sicurezza tecniche e organizzative relative agli applicativi in uso presso il Titolare.

5.3. Istanze degli Interessati

Tenendo conto della natura del trattamento, il Responsabile si obbliga ad assistere e supportare il Titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del CRC di dare riscontro alle richieste per l'esercizio dei diritti dell'interessato (negli ambiti e nel contesto del ruolo ricoperto e in cui opera il Responsabile).

In particolare, qualora il Responsabile riceva richieste provenienti dagli Interessati, finalizzate all'esercizio dei propri diritti, esso dovrà:

- darne tempestiva comunicazione scritta al Titolare, allegando copia delle richieste ricevute;
- coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni interne designate dal Titolare per gestire le relazioni con gli Interessati.

5.4. Autorizzati - Incaricati

Il Responsabile dovrà identificare e nominare le persone autorizzate ad effettuare operazioni di Trattamento sui dati di titolarità del CRC, identificando l'ambito autorizzativo consentito. Allo stesso tempo, il Responsabile dovrà:

- fornire agli Incaricati le dovute istruzioni relativamente alle operazioni ed alle modalità di Trattamento dei Dati Personali;

- rispettare e far rispettare agli autorizzati al trattamento e agli altri soggetti che per qualsivoglia motivo entreranno in contatto con i trattamenti di dati personali del CRC, le misure di sicurezza già attuate o che verranno in futuro predisposte ai sensi della normativa applicabile in materia di protezione dei dati personali;

- verificare con cadenza almeno annuale che i profili di accesso assegnati agli autorizzati al trattamento siano adeguati e non eccedenti alle esigenze della mansione.

Il Responsabile garantisce che i propri dipendenti e collaboratori siano affidabili ed abbiano piena conoscenza della normativa in materia di protezione dei dati personali. Ove non già presenti, il Fornitore deve documentare le istruzioni operative per il trattamento dei dati, comprensive delle misure da adottare per la sicurezza dei dati stessi.

6. Collaboratori esterni, sub-Responsabili e Terze Parti

Il Fornitore, previa autorizzazione scritta del CRC, potrebbe dover comunicare o rendere disponibili i Dati Personali di titolarità di quest'ultima ad uno o più soggetti terzi (quali sub-Responsabili) o a Collaboratori esterni, al fine di affidare a tali soggetti parte delle attività di Trattamento.

Il Fornitore è tenuto a comunicare preventivamente al Titolare la lista dei sub-Responsabili e Collaboratori Esterni di cui intende avvalersi, e ad impartire a tali soggetti, dietro autorizzazione espressa del CRC, precise istruzioni relativamente al Trattamento dei Dati Personali di titolarità del CRC.

Qualora opportuno al fine di dare attuazione alle previsioni del Regolamento UE 2016/679, del Codice Privacy e del Contratto in essere tra le Parti, il Responsabile, previa autorizzazione da parte del Titolare, si obbliga a far sottoscrivere ai propri sub-Responsabili e/o Collaboratori Esterni le medesime condizioni applicate nella presente designazione a responsabile, mediante sottoscrizione di appositi accordi con i sub-Responsabili e/o Collaboratori Esterni.

I Collaboratori Esterni e i sub-Responsabili potranno trattare i Dati Personali nella misura in cui tale trattamento sia strettamente necessario per l'esecuzione del Contratto che il Fornitore ha stipulato con il CRC, ed in ogni caso nel rispetto del presente accordo scritto, restando inteso tra le Parti che tali soggetti esterni saranno inoltre obbligati al rispetto delle limitazioni cui il Fornitore stesso è tenuto. Nello specifico, il Responsabile:

- si obbliga a stipulare con i Collaboratori Esterni e i sub-Responsabili un accordo scritto (o specifico atto di designazione a su-responsabili) che imponga a quest'ultimi il rispetto degli stessi obblighi in materia di protezione dei Dati Personali a cui il Responsabile è vincolato nei confronti del CRC (in base al Contratto e al presente atto di designazione), prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo che il trattamento soddisfi i requisiti della normativa italiana ed europea in materia di trattamento dei dati personali;
- si obbliga, in caso di autorizzazione scritta generale, ad informare il CRC di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri Collaboratori Esterni o sub-Responsabili del trattamento, dando così al Titolare del trattamento l'opportunità di opporsi a tali modifiche.

Qualora gli eventuali Collaboratori Esterni e sub-Responsabili del trattamento omettano di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile dichiara espressamente e garantisce di mantenere l'intera responsabilità circa l'adempimento degli obblighi da parte di tali soggetti.

Il Fornitore si impegna a non comunicare, trasferire o condividere, i Dati Personali di titolarità del CRC a Terze Parti.

7. Deroghe all'obbligo di riservatezza

Il Fornitore, i suoi dipendenti o i Collaboratori Esterni sono tenuti a non divulgare o comunicare i Dati Personali senza il consenso del CRC, fatta eccezione per l'ipotesi in cui detta comunicazione sia resa nei confronti di:

(a) soggetti autorizzati dal CRC, dipendenti del Fornitore o Collaboratori Esterni quando ciò sia necessario per l'esecuzione dei servizi, o
(b) una pubblica autorità competente, anche regolatoria e di vigilanza,

fermo restando che:

(i) la comunicazione di tali Dati Personali dovrà essere effettuata nel rispetto di questo accordo e della legge applicabile;
(ii) i contratti sottoscritti con i Collaboratori Esterni dovranno riportare le medesime previsioni di cui al presente documento relativamente al corretto trattamento e sulla riservatezza, e

(iii) il Fornitore e i Collaboratori Esterni dovranno dare al Titolare preventivo avviso scritto di comunicazioni conformi alla clausola 7 (b).

8. Comunicazione delle richieste di accesso, perdite o danno

Il Fornitore è tenuto a comunicare immediatamente al CRC e fornire tutta la necessaria assistenza:

(a) in caso di richiesta di accesso ai Dati Personali effettuata da un Interessato, da una autorità di controllo, da una autorità indipendente o dall'autorità giudiziaria;
(b) qualora venga a conoscenza di una delle seguenti circostanze, in conformità a quanto previsto nel precedente paragrafo 5.1:

i. Perdita, danneggiamento o distruzione dei Dati Personali;
ii. Accesso ai Dati Personali da parte di Terze Parti, fuori dai casi espressamente previsti dal Contratto;
iii. Qualunque circostanza o evento che possa determinare potenzialmente una violazione della normativa italiana ed europea in materia di protezione dei Dati Personali.

9. Attribuzione delle funzioni di amministratore di sistema *[U3]*

Il Responsabile deve assicurare la puntuale adozione delle misure di cui al Provvedimento dell'Autorità Garante per la protezione dei dati personali "Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" del 27 novembre 2008 e successive modifiche ed integrazioni.

In particolare, il Responsabile deve:

a) Provvedere alla designazione dei propri amministratori di sistema in forma scritta su base individuale, con elencazione analitica dell'ambito di operatività consentita in base al profilo di autorizzazione assegnata;
b) Stilare la lista degli amministratori di sistema e provvedere al relativo periodico aggiornamento. Tale lista dovrà includere gli estremi identificativi delle persone fisiche amministratori di sistema con l'elenco delle funzioni ad essi attribuite;
c) Fornire tempestivamente la lista aggiornata degli amministratori di sistema ogni qualvolta il Titolare ne faccia richiesta, anche tramite propri delegati e, in ogni caso, almeno una volta all'anno;
d) Garantire l'effettuazione di una verifica almeno annuale sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla legge per i Trattamenti di Dati Personali;
e) Adottare, anche relativamente ai software utilizzati, sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e degli archivi elettronici da parte degli amministratori di sistema. Le registrazioni devono:

- *avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste;*
- *comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate;*
- *essere conservate per un congruo periodo, comunque non inferiore a un anno e rese disponibili tempestivamente al Titolare, ogniqualvolta questi ne faccia richiesta, anche a mezzo di propri delegati.*

10. Controlli e attività di audit

Il Responsabile del trattamento si impegna a consentire al Titolare la verifica del rispetto della presente nomina e delle istruzioni fornite. Il Responsabile del trattamento si impegna a supervisionare e controllare direttamente i soggetti da esso designati per le operazioni di Trattamento ed a tal fine dovrà organizzare e curare la loro formazione.

Il Responsabile del trattamento inoltre riconosce al Titolare il diritto di effettuare attività di audit con cadenza annuale relativamente alle operazioni aventi ad oggetto il Trattamento dei Dati Personali di titolarità del CRC, avvalendosi di personale interno od esterno espressamente incaricato a tale scopo, anche presso le sedi del Responsabile.

Il Responsabile nominato, per i motivi su esposti, è obbligato a mettere a disposizione in qualunque momento e dietro richiesta del Titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina ed a contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Tali attività saranno effettuate dal Titolare periodicamente ed in base a metodologie concordate tra le Parti.

11. Durata e Cessazione del Trattamento

La presente nomina ha la medesima durata ed efficacia del Contratto in essere tra le Parti e, pertanto, cesserà al momento del completo adempimento o della cessazione del medesimo, qualsiasi ne sia il motivo. Il trattamento, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i Dati Personali sono stati raccolti e tali dati devono essere conservati nei sistemi e nelle banche dati del Responsabile in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello in precedenza indicato.

A seguito della cessazione del Trattamento affidato al Responsabile, nonché a seguito della cessazione del rapporto contrattuale sottostante, qualunque ne sia la causa, il Responsabile sarà tenuto (a discrezione e su specifica indicazione del Titolare) a:

(i) restituire al Titolare copia integrale dei Dati Personali trattati, e/o
(ii) provvedere alla loro integrale distruzione in modo che non siano più recuperabili, salvi solo i casi in cui la conservazione dei dati sia richiesta da norme di legge e/o altre finalità (contabili, fiscali, ecc.) o il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte del Responsabile, con modalità limitate e per il periodo di tempo a ciò strettamente necessario,
(iii) garantire in ogni caso la migrazione verso altro fornitore che sarà indicato dal CRC, consentendo così la portabilità di tutti i dati trattati.

12. Accordo relativo al trasferimento dei dati all'estero

Il Responsabile si impegna a circoscrivere gli ambiti di circolazione e trattamento dei Dati Personali (es. memorizzazione, archiviazione e conservazione dei dati sui propri server) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 (Paese terzo giudicato adeguato dalla Commissione europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.).

Il Fornitore, pertanto, non dovrà trasferire o effettuare il trattamento dei Dati Personali del CRC al di fuori dell'Unione Europea, per nessuna ragione, in assenza di autorizzazione scritta del CRC. Qualora il CRC rilasci l'autorizzazione di cui al presente paragrafo e venga pertanto effettuato un trasferimento dei Dati Personali del CRC al di fuori dell'Unione Europea, tale trasferimento dovrà rispettare le previsioni di cui al Regolamento UE 2016/679 sopra indicate.

Resta inteso tra le Parti che il Fornitore dovrà garantire che i metodi di trasferimento impiegati, ivi inclusa la conformità alle clausole contrattuali standard approvate dalla Commissione Europea e sulla base dei presupposti indicati nella medesima decisione, consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata del presente Contratto.

Il Fornitore è obbligato a comunicare immediatamente al CRC il verificarsi di una delle seguenti fattispecie:

(a) mancato rispetto delle clausole contrattuali standard di cui sopra, oppure
(b) qualsiasi modifica della metodologia e delle finalità di trasferimento dei Dati Personali del CRC all'estero.

13. Manleva e Responsabilità per violazione delle disposizioni

Il Responsabile, con l'accettazione della presente nomina, si impegna a mantenere indenne il Titolare da qualsiasi responsabilità, danno, incluse le spese legali, o altro onere che possa derivare da pretese, azioni o procedimenti avanzate da terzi a seguito dell'eventuale illiceità o non correttezza delle operazioni di trattamento dei Dati Personali che sia imputabile a fatto, comportamento o omissione del Responsabile (o di suoi dipendenti e/o Collaboratori esterni).

Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico.

Fatti salvi gli articoli 82, 83 e 84 del Regolamento UE 2016/679, in caso di violazione delle disposizioni contenute nella presente nomina relative alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute o in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile dal Regolamento UE 2016/679, il Responsabile sarà considerato quale Titolare del trattamento e ne risponderà direttamente dal punto di vista sanzionatorio.

14. Accettazione della nomina

Con la sottoscrizione del presente atto, ai sensi della Normativa in materia di Protezione dei Dati Personali, il Responsabile accetta la propria nomina, in relazione ai dati personali la cui conoscenza risulta essere indispensabile per l'adempimento delle obbligazioni di cui al Contratto. Il Responsabile è a conoscenza degli obblighi previsti dal Regolamento UE 2016/679 e dal D.lgs. 196/2003 (e s.m.i.) e dovrà attenersi per lo svolgimento dei compiti assegnatigli alle previsioni ed ai compiti contenuti nel presente atto di nomina.

Napoli, _____

Il Titolare del Trattamento

_____

Il Responsabile del trattamento

_____

ACCORDO PER LA PROTEZIONE DEI DATI PERSONALI E
DESIGNAZIONE A RESPONSABILE ESTERNO DEL TRATTAMENTO

Il Consiglio regionale della Campania, con sede in Napoli Centro Direzionale, Isola F13 – 80143, Codice Fiscale e P. IVA 80051460634 (di seguito la "**CRC**" o il "**Titolare**"), in qualità di Titolare del trattamento ai sensi del Regolamento UE 2016/679 (di seguito "**GDPR**"), in persona del Presidente, dr.ssa Rosa D'Amelio.

E

_____*inserire nome ditta***_____**, con sede legale _____, in persona del legale rappresentante pro tempore (di seguito "**Fornitore**" o "**Responsabile**")

Congiuntamente indicate come le "**Parti**".

PREMESSO CHE

- Nell'esecuzione delle Vostre attività, derivanti dal "contratto di _____" ("Contratto") con Voi sottoscritto in data ___/___/_____ sono coinvolte operazioni di trattamento di dati personali effettuate per nostro conto, di cui CRC è Titolare;

CONSIDERATO CHE

- Data l'attività e la Vs. specializzazione professionale, sussistono i requisiti di esperienza, capacità e affidabilità prescritti dalla normativa rilevante in materia di protezione dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nel trattamento dei dati personali.

Tanto premesso e considerato, CRC, in qualità di Titolare per il Trattamento,

CON IL PRESENTE ATTO DESIGNA

Il Sig./Sig.ra/dott._____ (di seguito anche "Responsabile"), come sopra rappresentato, responsabile esterno dei trattamenti dei dati personali, limitatamente ed esclusivamente agli obblighi derivanti dal contratto concluso tra le parti.

DISCIPLINA DEI TRATTAMENTI DA ESEGUIRE PER CONTO DEL TITOLARE

- Con riguardo alla disciplina dei trattamenti da eseguire per conto del Titolare, in relazione alla durata, alla natura ed alla finalità del trattamento, al tipo di dati personali trattati ed alle categorie di interessati, agli obblighi ed ai diritti del Titolare del trattamento, per quanto non specificato all'interno della presente nomina, si rinvia integralmente al contratto intercorrente tra le parti;
- con riguardo alla disciplina dei trattamenti da eseguire per conto del Titolare, si specificano i seguenti parametri:

Trattamenti da effettuare per conto del Titolare	Trattamento elettronico e cartaceo dei dati personali connesso alla erogazione dei servizi di ……, limitatamente e con esclusivo riferimento agli obblighi da contratto derivanti, ivi compreso il profilo relativo alla sicurezza di cui all'art. 32 del Regolamento Europeo n. 679/2016 (in relazione al quale si rammenta che il trattamento dovrà avvenire in modo da garantire la sicurezza, la riservatezza, disponibilità e l'integrità dei dati di titolarità del CRC).

Materia disciplinata	……
Durata del trattamento	I trattamenti avranno luogo per l'arco di tempo corrispondente alla durata del contratto in essere tra le parti o fino al raggiungimento delle finalità dallo stesso perseguite (come in seguito specificato).
Finalità del trattamento	……
Tipo di dati personali e Categorie di interessati	La tipologia dei dati personali trattati dal Responsabile, in riferimento ai servizi espletati e per i quali viene autorizzato, può includere: *dati personali di natura comune relativi a persone fisiche identificate o identificabili, categorie particolari di dati (es. stato di salute o appartenenza sindacale), etc.* Tali dati personali si riferiscono alle seguenti categorie di interessati: ……

GARANZIE E OBBLIGHI DEL RESPONSABILE

A seguito di tale nomina il Responsabile:

- si obbliga a prestare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento svolto per conto del Titolare soddisfi i requisiti del Regolamento Europeo in materia di protezione dei dati personali delle persone fisiche (Regolamento Europeo n. 679/2016), garantendo inoltre la tutela dei diritti dell'interessato;
- garantisce che i propri hardware ed i software coinvolti ed utilizzati nel trattamento consentano il rispetto dei principi della Privacy by Design e della Privacy by Default;
- si obbliga, qualora intenda ricorrere ad un altro responsabile ("sub-responsabili") per lo svolgimento di una o più attività relative al contratto sottoscritto, ad informare CRC e, salvo non sia stato già diversamente pattuito, richiederne preventivamente allo stesso un'autorizzazione scritta (specifica o generale);
- si obbliga a stipulare con i terzi sub-responsabili un accordo scritto (nomina) o contratto che imponga a quest'ultimi il rispetto degli stessi obblighi in materia di protezione dei dati a cui il Responsabile è vincolato nei confronti del CRC (in base alla presente nomina), prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo che il trattamento soddisfi i requisiti della normativa italiana ed europea in materia di trattamento dei dati personali;
- si obbliga, in caso di autorizzazione scritta generale, ad informare CRC circa il 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;
- qualora gli eventuali sub-responsabili del trattamento omettano di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile dichiara espressamente e garantisce di mantenere nei confronti della filiera dei sub-responsabili l'intera responsabilità dell'adempimento degli obblighi di tali soggetti terzi;
- si obbliga a trattare 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 deve

informare CRC circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

- garantisce che in qualsiasi attività di trattamento di dati personali venga impiegato esclusivamente personale autorizzato (es. collaboratori e/o colleghi), che operi sotto la diretta autorità del Responsabile ed, a tal proposito, si impegna a formarlo ed istruirlo (anche per iscritto), vigilando sulla puntuale applicazione delle istruzioni impartite;
- garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- si impegna a circoscrivere gli ambiti di circolazione e trattamento dei dati personali (es. memorizzazione, archiviazione e conservazione dei dati su server o in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal GDPR n. 679/2016 (Paese terzo giudicato adeguato dalla Commissione europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.);
- si impegna a interagire con il Garante per la protezione dei dati personali, in caso di richiesta di informazioni o effettuazione di controlli e accessi da parte dell'Autorità.

ADOZIONE DELLE MISURE DI SICUREZZA E MISURE TECNICHE ORGANIZZATIVE

Per quanto riguarda le misure organizzative e di sicurezza, il Responsabile:

- si obbliga a adottare tutte le misure di cui all'art. 32 del Regolamento Europeo n. 679/2016 in modo da garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati, tenendo conto dei provvedimenti tempo per tempo emanati dall'Autorità Garante per la protezione dei dati personali italiana inerenti ai trattamenti svolti dal Responsabile. Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito;
- si impegna a provvedere alla gestione, monitoraggio, messa in sicurezza ed aggiornamento dei propri sistemi informativi (anche nel caso in cui ci si avvalga di soggetti terzi per l'infrastruttura IT) sui quali siano eventualmente presenti dati personali di titolarità del CRC, nonché verificare il corretto funzionamento e controllo dei sistemi sui quali poggiano tali informazioni e dati personali;
- si impegna ad adottare sui propri sistemi e su quelli del CRC adeguati sistemi di protezione (programmi antivirus, firewall ed altri strumenti software o hardware) atti a garantire la massima sicurezza, utilizzando le conoscenze acquisite in base al progresso tecnico e verificandone l'installazione, l'aggiornamento ed il funzionamento degli stessi;
- si obbliga a predisporre ed implementare le eventuali ed ulteriori misure di sicurezza nell'eventualità di un trattamento elettronico di "categorie particolari di dati" (es. dati sensibili) ovvero di dati giudiziari;
- si impegna a mantenere un elenco, da aggiornare con cadenza annuale, di tutte le attrezzature informatiche (HW e SW) utilizzate per il trattamento dei dati di titolarità del CRC, dello scopo a cui sono destinate, della loro allocazione fisica, delle misure di sicurezza sulle stesse adottate e delle eventuali misure di adeguamento pianificate;
- si impegna, per tutto il periodo del trattamento, a custodire i dati personali in ambiente sicuro e protetto con criteri di sicurezza e separazione tali da non consentire l'accesso a persone non autorizzate al trattamento;
- si obbliga ad informare prontamente CRC di ogni questione rilevante ai fini di legge o di sicurezza e dare tempestiva notizia al medesimo di eventuali richieste che dovessero pervenirgli da parte

dell'Autorità di controllo competente e/o da parte degli interessati;

- si impegna a adottare politiche interne e meccanismi atti a garantire e dimostrare il rispetto della privacy e predisporre, a richiesta del CRC, rapporti scritti in merito agli adempimenti eseguiti ai fini di legge e alle conseguenti risultanze;
- si impegna ad assistere il Titolare del trattamento, relativamente ai dati oggetto di trattamento da parte del Responsabile, nel garantire il rispetto degli obblighi relativi:
  - alla sicurezza del trattamento;
  - alla notifica di una violazione dei dati personali all'Autorità di controllo;
  - alla comunicazione di una violazione dei dati personali all'interessato;
  - alla valutazione d'impatto sulla protezione dei dati;
  - alla consultazione preventiva.

In particolare, in caso di violazione dei dati personali che ne determini la distruzione, perdita, modifica, divulgazione non autorizzata dei dati personali, il Responsabile deve:

- informare CRC, tempestivamente e senza ingiustificato ritardo, di essere venuto a conoscenza di una violazione e fornire tutti dettagli completi della violazione subita (descrizione, volume dei dati personali interessati, natura della violazione, i rischi per gli interessati e le misure adottate per mitigare i rischi);
- fornire assistenza al CRC per far fronte alla violazione e alle sue conseguenze (soprattutto in capo agli interessati coinvolti).

I suindicati obblighi sono adempiuti alla luce della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento.

ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Tenendo conto della natura del trattamento, il Responsabile si obbliga ad assistere e supportare il Titolare del trattamento con misure tecniche e organizzative adeguate, per le attività di trattamento delegate e i dati degli interessati comunicati, al fine di soddisfare l'obbligo del CRC di dare seguito alle richieste per l'esercizio dei diritti dell'interessato (negli ambiti e nel contesto, ovviamente, del ruolo ricoperto e in cui opera il Responsabile).

DURATA E CESSAZIONE DEL TRATTAMENTO

Il presente atto di designazione a responsabile esterno del trattamento è produttivo di effetti per tutta la durata del rapporto contrattuale in essere tra CRC ed il Responsabile e, pertanto, alla cessazione definitiva di questo rapporto lo stesso decadrà con effetto immediato. Il trattamento, pertanto, deve avere una durata non superiore a quella necessaria agli scopi per i quali i dati personali sono stati raccolti e tali dati devono essere conservati nei sistemi del Responsabile in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello in precedenza indicato.

In caso di cessazione dei rapporti in essere o comunque al termine della prestazione dei servizi relativi al trattamento, il Responsabile si impegna, su richiesta e sulla base delle istruzioni che riceverà dal Titolare, a restituire tutti i dati personali conferiti e ad eliminare (in modo permanente e irreversibile) tali dati e le eventuali copie esistenti, esclusi i casi in cui specifiche norme di legge ne prevedano la conservazione o il caso in cui si verifichino circostanze autonome e ulteriori che giustifichino la continuazione del trattamento dei dati da parte del Responsabile, con modalità limitate e per il periodo di tempo a ciò strettamente necessario.

OBBLIGHI E DIRITTI DEL TITOLARE

CRC ha diritto di ottenere dal Responsabile tutte le informazioni (relative alle misure organizzative e di sicurezza) necessarie per verificare l'affidabilità e dimostrare il rispetto delle istruzioni e degli obblighi affidati allo stesso o derivanti dalla normativa italiana ed europea.

A tal fine, CRC ha il diritto di disporre - a propria cura e spese - verifiche a campione o specifiche attività di audit o di rendicontazione in ambito privacy e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile.

Il Responsabile nominato, per i motivi su esposti, è obbligato a mettere a disposizione in qualunque momento e dietro richiesta del Titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina e a contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Qualora il Responsabile rilevi che un'istruzione impartita dal Titolare violi le disposizioni relative alla normativa rilevante in tema di protezione dei dati, si obbliga ad informare immediatamente lo stesso di tale circostanza.

VIOLAZIONE DELLE DISPOSIZIONI

Fatti salvi gli articoli 82, 83, 84, del Regolamento Europeo n. 679/2016, in caso di violazione delle disposizioni contenute nella presente nomina relative alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute o in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile dal Regolamento Europeo n. 679/2016, il Responsabile sarà considerato quale Titolare del trattamento.

ACCETTAZIONE DELLA NOMINA

Con la sottoscrizione del presente atto, ai sensi dell'art. 28 del Regolamento Europeo n. 679/2016, il Responsabile esterno del trattamento accetta la propria nomina, in relazione ai dati personali la cui conoscenza risulta essere indispensabile per lo svolgimento delle obbligazioni di cui al contratto in essere tra le parti. Il Responsabile è a conoscenza degli obblighi previsti dal Regolamento Europeo n. 679/2016 e dovrà attenersi per lo svolgimento del compito assegnatogli alle previsioni ed ai compiti contenuti nel presente atto di nomina.

Vi preghiamo di restituirci la presente firmata per accettazione in ogni sua pagina.

IL TITOLARE DEL TRATTAMENTO **IL RESPONSABILE DEL TRATTAMENTO**

_____ _____

Responsabile	Ambito di responsabilità	Estremi contrattuali	
			Lettera di designazione art. 28/GDPR del ……. – clausole contrattuali
			Accordo sulla protezione dei dati (designazione art. 28 GDPR del ……).
			Accordo sulla protezione dei dati
			Lettera di designazione art. 28/GDPR del …….
			Lettera di designazione art. 28/GDPR del …….
			Lettera di designazione art. 28.