



Regolamento *Privacy* Aziendale

Kratos società cooperativa

Data approvazione	03.09.2018
Data modifica	01.08.2019
Data modifica	01.09.2020
Data modifica	01.10.2021
Data modifica	09.09.2022
Data modifica	20.11.2023

L'ultima revisione sostituisce qualsiasi revisione precedente.

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

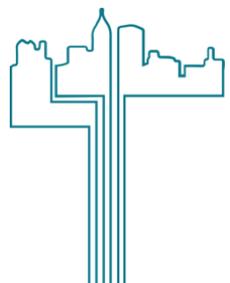
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237

Member of CISQ Federation



CQOP SOA
CONSTRUTTORI QUALIFICATI OPERE PUBBLICHE





Sommario

<u>1. PREMESSE E NORMATIVA APPLICABILE</u>	4
<u>2. OGGETTO E FINALITÀ DEL REGOLAMENTO PRIVACY AZIENDALE</u>	4
<u>3. AMBITO DI APPLICAZIONE DEL REGOLAMENTO</u>	5
<u>4. AUTORITÀ DI CONTROLLO COMPETETE E GIURISDIZIONE</u>	5
<u>5. DEFINIZIONI</u>	5
<u>6. DATI TRATTATI E BASI GIURIDICHE DEL TRATTAMENTO DEI DATI PERSONALI</u>	6
6.1. VIDEOSORVEGLIANZA	7
<u>7. PERIODO DI CONSERVAZIONE DEI DATI PERSONALI</u>	9
<u>8. TRATTAMENTO DEI DATI PERSONALI DA PARTE DI TERZI E TRASFERIMENTO DATI EXTRA-UE</u>	10
<u>9. MISURE TECNICHE E ORGANIZZATIVE ADOTTATE</u>	10
10. PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA	10
11. MISURE DI SICUREZZA ORGANIZZATIVE E TECNICHE ADOTTATE	10
12. REGISTRO ELETTRONICO DELLE ATTIVITÀ DI TRATTAMENTO	11
<u>13. NOMINA DEL RESPONSABILE DEL TRATTAMENTO</u>	12
<u>14. MODELLO ORGANIZZATIVO <i>PRIVACY</i></u>	12
<u>15. LINEE GUIDA PER GLI INCARICATI DEL TRATTAMENTO</u>	13
15.1. OBBLIGHI DEGLI INCARICATI	13
15.2. MODALITÀ DI SVOLGIMENTO DELLE OPERAZIONI DEGLI INCARICATI	14
15.3. ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI	14
15.4. ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"	18

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

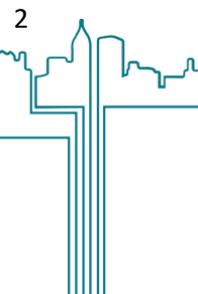
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237

Member of CISQ Federation



CQOP SOA
COSTRUTTORI QUALIFICATI OPERE PUBBLICHE





<u>16. LINEE GUIDA PER GLI ADDETTI ALLA MANUTENZIONE</u>	19
<u>17. SANZIONI</u>	21
<u>18. ENTRATA IN VIGORE DEL REGOLAMENTO E PUBBLICITÀ</u>	21
<u>19. AGGIORNAMENTO E REVISIONE</u>	21
<u>ALLEGATO 1. NOMINA DEGLI INCARICATI DEL TRATTAMENTO</u>	21
<u>ALLEGATO 2 NOMINA DEL PREPOSTO ALLA CUSTODIA DELLE PAROLE CHIAVE</u>	21
<u>ALLEGATO 3 – LINE GUIDA E MODULO PE L’ESERCIZIO DEI DIRITTI DELL’INTERESSATO</u>	21

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

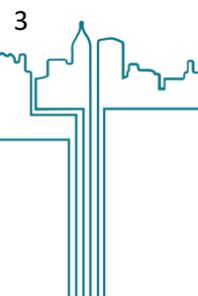
Tel.: 0683970237

Member of CISQ Federation



CERTIFIED MANAGEMENT SYSTEM
ISO 9001

CQOP SOA
COSTRUTTORI QUALIFICATI OPERE PUBBLICHE





1. Premesse e normativa applicabile

Il presente Regolamento *privacy* aziendale è predisposto in conformità con la normativa in materia di protezione dei dati personali e, in particolare:

- **D.lgs. 30 giugno 2003, n. 196**, come novellato dal **D.lgs. 10 agosto 2018 n. 101**, Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) n. 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 (c.d. Codice *privacy*);
- **Reg. 2016/679/UE**, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione europea il 4 maggio 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, in inglese *General Data Protection Regulation*, c.d. GDPR);
- Artt. 7 e 8, **Carta dei diritti fondamentali dell'Unione Europea**;
- Art. 8, **Carta Europea dei Diritti dell'Uomo (CEDU)**.

A far data dal 25 maggio 2018 ha trovato diretta ed immediata applicazione, sul territorio nazionale, il nuovo Reg. 2016/679/UE (d'ora in poi "GDPR"). Ciò ha comportato la necessità di integrare le disposizioni legislative di cui al previgente Codice *privacy* (D.lgs. 196/2003) attuata con il D.lgs. 101/2018 di adeguamento al GDPR), così come delle norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, nella misura in cui le norme nazionali risultino contrastanti o incompatibili con quelle europee.

Il principio cardine, di matrice anglosassone, introdotto dal nuovo Regolamento Europeo è quello della **responsabilizzazione (*accountability*)** che pone in capo al Titolare del trattamento dei dati (di seguito anche solo "Titolare") l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee, in applicazione del generale **principio della conformità (*compliance*)**.

Nell'ottica del Legislatore europeo, quindi, in materia di *privacy* ciascun Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto egli risponde delle proprie azioni e deve essere in grado, in qualsiasi momento, di darne conto prova.

2. Oggetto e finalità del Regolamento *privacy* aziendale

Il presente Regolamento *privacy* aziendale disciplina, all'interno della Società Cooperativa KRATOS, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dalla normativa vigente sopra citata.

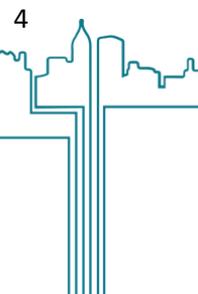
KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237





KRATOS, in qualità di Titolare del trattamento e di Responsabile del trattamento, garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale.

3. Ambito di applicazione del regolamento

Il Regolamento *privacy* aziendale si applica a tutti i lavoratori, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

4. Autorità di controllo competete e giurisdizione

L'Autorità di controllo e l'autorità giudiziale competente sono quelle dello Stato membro della UE avente il legame più stretto con il trattamento dei relativi dati personali.

5. Definizioni

Si rinvia a all'art. 4 del GDPR per le definizioni utilizzate. A queste si aggiungono le seguenti definizioni:

- **DPO (Data Protection Officer – Il Responsabile della protezione dei dati):** Il responsabile della protezione dei dati GDPR;
- **Incaricati al trattamento dati:** dipendenti e collaboratori del Titolare che compiono materialmente il trattamento dei dati personali (per conto del Titolare). Indica il ruolo del soggetto che ha accesso ai dati personali ed agisce sotto l'autorità del Titolare o del Responsabile, dietro specifiche istruzioni da parte di costoro.
- **Interessati al trattamento:** I soggetti di cui si acquisiscono i dati personali; Per i diritti dell'Interessato si rinvia alle linee guida e al modulo per l'esercizio dei diritti dell'interessato.
- **Registro Data Breach:** registro delle violazioni dei dati personali che è unico ed è tenuto dal Titolare il quale definisce i criteri e le modalità della tenuta, gestione e accessibilità delle informazioni ivi contenute, in modo tale da garantire facile accesso, gestione, consultazione, estrazione e stampa delle stesse. Il Titolare è tenuto ad aggiornare tempestivamente il Registro *Data Breach* ogni qualvolta sia comunicata una variazione del suo contenuto, in linea con le disposizioni di cui alla Procedura *Data Breach* di KRATOS.
- **Referente *privacy*:** soggetto con funzioni di coordinamento dell'attuazione della

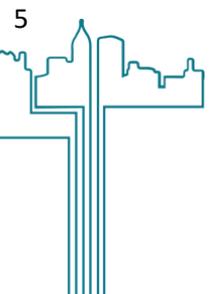
KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237





procedura *Data Breach*, il quale sarà nominato nel caso di violazione dei dati personali.

6. Dati trattati e basi giuridiche del trattamento dei dati personali

I dati trattati sono dati personali rientranti nelle seguenti categorie:

- Dati anagrafici (nome e cognome, data e luogo di nascita, città e indirizzo di residenza o domicilio)
- Dati identificativi (es. C.F., P.IVA., dati catastali)
- Dati di contatto (es. indirizzo email, numero di telefono/cellulare)
- Dati relativi al/ai contratti di lavoro, collaborazione o fornitura
- Dati fiscali, contabili o bancari (es. regime previdenziale, TFR, estremi conto corrente bancario)
- Copia per immagine di documenti di riconoscimento;
- Dati delle immagini audiovisive delle telecamere di sorveglianza.

Il GDPR sancisce che ogni trattamento deve trovare fondamento in un'adeguata base giuridica. I fondamenti di liceità del trattamento sono indicati all'art. 6 GDPR.

In particolare, le basi giuridiche del trattamento sono:

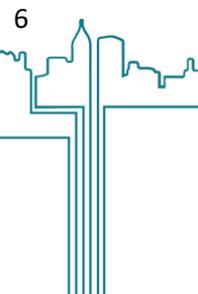
- Il **consenso dell'interessato** c.d. consenso *privacy* (art. 6, par. 1, lett. a), GDPR), espresso secondo le condizioni di cui all'art. 7 GDPR. In particolare, il consenso dell'interessato per iscritto a seguito della somministrazione dell'Informativa sul trattamento dei dati personali redatta in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento - con la stessa facilità con cui è accordato - ma la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.
- L'**esecuzione di un contratto** di cui l'interessato è parte o di misure precontrattuali adottate su richiesta dell'interessato, c.d. consenso contrattuale, (art. 6, par. 1, lett. b), GDPR), limitatamente a quei dati necessari per l'esecuzione di un contratto;
- L'**adempimento di un obbligo legale** da parte del Titolare o del Responsabile (art. 6, par. 1, lett. c), GDPR);
- **esecuzione di un compito di interesse pubblico** o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e), GDPR)
- Il **legittimo interesse** del Titolare del trattamento o di terzi ad effettuare trattamenti necessari alle finalità indicate (art. 6, par. 1, lett. f), GDPR).

Tutte le comunicazioni relative alla tutela dei dati personali, effettuate a mezzo posta elettronica sono effettuate tramite l'indirizzo email privacy@coopkratos.it; mentre quelle effettuate tramite posta elettronica certificata, sono effettuate attraverso la pec kratos.coop@legalmail.it.

Sono trattati dati personali rientranti nel novero delle **particolari categorie di dati** di cui all'**art. 9 GDPR**. Essi riguardano esclusivamente:

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





a) la procedura di verifica del Green Pass dei lavoratori, collaboratori e soggetti terzi che intendono accedere ai locali di KRATOS e sono: l'informazione relativa al possesso del Green Pass valido o la certificazione medica di esonero dalla campagna vaccinale per COVID19 e, in generale, lo stato di salute con particolare riguardo al COVID-19. Tali dati sono trattati conformemente alle seguenti basi giuridiche:

- assolvimento degli obblighi ed esercizio di diritti specifici del Titolare del trattamento e dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale su autorizzazione del diritto europeo e nazionale italiano (art. 9, par. 2, lett. b), GDPR)
- motivi di interesse pubblico rilevante sulla base del diritto Europeo e nazionale italiano, proporzionato alla finalità perseguita e nel rispetto dell'essenza del diritto alla protezione dei dati, con la previsione di misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. g), GDPR).

I dati particolari sopra elencati sono trattati fino al termine dello stato d'emergenza previsto dalle autorità pubbliche competenti.

b) la procedura di organizzazione, gestione e controllo ex D.Lgs n. 231/2001 per prevenire la commissione dei reati disciplinati dallo stesso D.Lgs.

Tali dati sono trattati conformemente alle seguenti basi giuridiche:

- assolvimento degli obblighi ed esercizio di diritti specifici del Titolare del trattamento e dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale su autorizzazione del diritto europeo e nazionale italiano (art. 9, par. 2, lett. b), GDPR)
- motivi di interesse pubblico rilevante sulla base del diritto Europeo e nazionale italiano, proporzionato alla finalità perseguita e nel rispetto dell'essenza del diritto alla protezione dei dati, con la previsione di misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9, par. 2, lett. g), GDPR).

I dati particolari sopra elencati sono trattati fino al termine della procedura di verifica.

Tutte le informazioni sulla procedura ai sensi del D.Lgs n. 231/2001 e ss.mm.ii. sono riportate nel manuale di organizzazione gestione e controllo con i relativi allegati e le relative appendici, incluso il Codice Etico, ai quali si rinvia integralmente.

Tutte le comunicazioni relative alla procedura di organizzazione, gestione e controllo ex D.Lgs n. 231/2001 sono effettuate tramite l'**email dedicata**: comunicazioni231@coopkratos.it

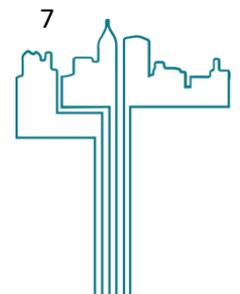
6.1. Videosorveglianza

Presso la sede del Titolare è in funzione un **sistema di videosorveglianza** locale, per garantire **adeguati livelli di sicurezza delle risorse umane e dei beni materiali ed immateriali ivi presenti**.

Il trattamento dei dati personali avviene tramite il rilevamento dei sistemi di videosorveglianza. Le riprese audio-video vengono raccolte attraverso il sistema di videosorveglianza e sono

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





visionate dagli addetti ai controlli allo scopo di monitorare gli ingressi e garantire un adeguato livello di sicurezza del personale e dei beni del Titolare.

Le riprese vengono, registrate mediante appositi sistemi informatizzati e vengono **conservate per il periodo di massimo 72 ore (tre giorni)**, decorso il quale vengono cancellate. Tale periodo di conservazione è conseguenza del fatto che il sabato e la domenica le attività lavorative del Titolare del trattamento sono chiuse e, pertanto, è necessario lasciare attive le telecamere durante tutto il fine settimana (sia la giornata di sabato che quella di domenica). Al rientro in sede le immagini vengono cancellate, previa visione dei filmati e accertata l'assenza di violazioni alla sicurezza del personale e dei beni del Titolare. La durata della registrazione per 72 ore è quindi attuata nel pieno **rispetto di minimizzazione dei trattamenti bilanciata dal legittimo interesse del Titolare** a mantenere le registrazioni delle telecamere attive per le due giornate di sabato e domenica in cui le attività lavorative del Titolare sono chiuse e non vi è personale in sede che può svolgere le consuete attività di verifica e cancellazione dei dati.

I dati personali vengono trattati nel rispetto del GDPR, del codice privacy e dello Statuto dei lavoratori (L. n. 300/1970), nonché delle Linee guida sul trattamento dei dati personali tramite dispositivi video n. 3/2019 del Comitato Europea per la Protezione dei Dati (EDPB), e del provvedimento del Garante per la Protezione dei Dati Personali in materia di videosorveglianza dell'8.04.2010.

Nel rispetto del divieto di cui all'art. 4 dello Statuto dei lavoratori, **la videosorveglianza non può mai essere utilizzata per effettuare controlli a distanza sull'attività lavorativa** dei lavoratori, collaboratori o altri soggetti che a qualsiasi titolo svolgano anche occasionalmente la loro attività lavorativa presso i locali del Titolare.

Le riprese non sono in alcun modo impiegate come strumento di sorveglianza e monitoraggio a distanza del personale, degli utenti camerali e in genere degli interessati che transitano nelle aree videoriprese.

L'impianto di videosorveglianza non può essere utilizzato per finalità statistiche, nemmeno se consistenti nella raccolta aggregata dei dati.

L'attività di videosorveglianza raccoglie solo i dati strettamente necessari per il raggiungimento delle finalità perseguite e sopra definite nel rispetto dei **principi di pertinenza e non eccedenza**. La localizzazione delle telecamere, l'angolo di visuale e le modalità di ripresa sono stabilite in modo da garantire la minimizzazione dei dati oggetto di trattamento. Viene inoltre evitata l'installazione di strumenti di videosorveglianza in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorra un'effettiva esigenza di deterrenza.

Gli strumenti di videoripresa vengono, pertanto, installati:

- esternamente, per la sorveglianza del perimetro esterno degli edifici e delle porte di accesso;

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

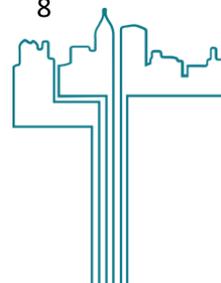
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237

Member of CISQ Federation



CQOP SOA
COSTRUTTORI QUALIFICATI OPERE PUBBLICHE





- internamente per la sorveglianza delle aree interne quali magazzino e aree di transito con accesso anche da parte di soggetti esterni autorizzati. Le telecamere installate internamente si attivano con il movimento e la ripresa dura per 10 (dieci) secondi.

In corrispondenza di ogni telecamera attiva è affisso un **cartello** con tutte le indicazioni essenziali relative al trattamento dei dati personali tramite il sistema di videosorveglianza. La **relativa informativa completa sul trattamento di tali dati personali** è disponibile presso i locali del Titolare (bacheca) e online scansionando il QR code riportato sul cartello stesso.

Il Titolare e il Responsabile, anche per il tramite dei rispettivi incaricati, si impegnano ad adottare tutte le **misure di sicurezza secondo quanto previsto dall'art. 32 del GDPR**, al fine di ridurre i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. In particolare, il Titolare e il Responsabile si impegnano ad applicare il **principio di minimizzazione dei dati**, trattando solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (art. 5, par. 1, lett. c), GDPR).

7. Periodo di conservazione dei dati personali

In applicazione del principio di **minimizzazione del trattamento**, sono trattati solo i dati necessari e per il periodo di tempo necessario.

In particolare, i dati personali sono trattati per il **tempo necessario all'esecuzione del contratto** di cui l'Interessato è parte in qualità di dipendente, fornitore o collaboratore del Titolare, nonché di soggetto terzo che intende accedere ai locali del Titolare o entrare in contatto con il Titolare.

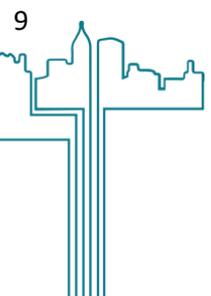
I dati sono trattati, altresì, per il **tempo necessario all'adempimento di un obbligo legale** a cui il Titolare o il Responsabile sono soggetti, ovvero **all'esercizio di un legittimo interesse del Titolare o di terzi**.

Nel caso di dati trattati tramite le telecamere di **videosorveglianza**, la conservazione dei dati dura per **massimo 74 ore**. Dopo tale termine, le registrazioni vengono cancellate, salvo che le stesse non siano necessarie per l'espletamento di indagini atte a verificare la sicurezza delle risorse umane e dei beni del Titolare.

Una volta cessato il rapporto di lavoro con i relativi Incaricati del Trattamento o Responsabili del trattamento del Titolare, questi non hanno più la facoltà di accedere ai dati personali trattati nell'esercizio delle proprie attività e hanno il divieto di diffondere i dati che sono stati in loro possesso durante l'esercizio delle proprie attività. Per assicurare che gli Incaricati non siano più in grado di accedere a tali dati, vengono cambiate periodicamente le credenziali di accesso dei sistemi informatici contenenti i dati – grazie al supporto del preposto alla custodia delle parole chiave e – e impedito l'accesso alla sede e, in particolare, ai locali del Titolare.

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





8. Trattamento dei dati personali da parte di terzi e trasferimento dati extra-UE

Non sono in atto trattamenti dei dati al di fuori dell'Unione Europea (trattamenti extra-UE). Tuttavia, sono state ugualmente previste **procedure formali relative agli eventuali casi di trattamento dei dati personali extra-UE da parte di Terze Parti**, i quali sono ben definiti, documentati e concordato tra il Titolare del trattamento e la Terza Parte prima dell'inizio delle attività di trattamento.

L'organizzazione del Titolare del trattamento svolge regolarmente audit per controllare il permanere della conformità dei trattamenti affidati ai Responsabili del trattamento ai livelli e alle istruzioni conferite per il pieno rispetto dei requisiti e obblighi.

In ogni caso, il **trasferimento dei dati extra-UE** sarà eventualmente possibile solo in casi espressamente determinati e solo:

- verso un Paese terzo il cui livello di protezione dei dati personali è considerato adeguato ai sensi delle decisioni assunte dalla Commissione europea (art. 45, GDPR),
- oppure sulla base di garanzie adeguate e a condizione che gli interessati del trattamento godano di diritti azionabili e mezzi di ricorso effettivi secondo quanto previsto dall'art. 46 GDPR,
- oppure di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 GDPR.

9. Misure tecniche e organizzative adottate

10. Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

L'art. 25 GDPR introduce il criterio sintetizzato dall'espressione inglese "**data protection by default and by design**", ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio e per impostazione predefinita le garanzie indispensabili al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tali attività di protezione dei dati personali avvengono sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso. Ciò richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

Le misure tecniche e organizzative adottate dal Titolare, anche nel rispetto dei principi di cui all'art. 25 GDPR sono descritte nel seguente sotto-paragrafo.

11. Misure di sicurezza organizzative e tecniche adottate

Il titolare ha adottato le seguenti misure preventive di natura sia organizzativa che tecnica per la tutela dei dati personali:

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237





a) Misure organizzative:

- nomina per iscritto del personale;
- istruzioni, formazione e sensibilizzazione degli Incaricati al trattamento;
- accesso controllato ai sistemi informatici tramite credenziali di accesso adeguate;
- archiviazione cartacea in armadi chiusi e accessibili solo al personale autorizzato;
- archivi digitali su server remoti;
- *Privacy Policy* aziendale;
- Procedura *Data Breach*.

b) Misure tecniche:

- Autenticazione prima dell'accesso digitale o cartaceo ai dati;
- criteri prestabiliti da rispettare per la generazione di sicure credenziali di accesso ai sistemi informatici;
- procedura di modifica periodica delle credenziali di accesso;
- firewall;

antivirus per evitare problematiche relative a virus o malware (*L'antivirus installato è l'antivirus di WINDOWS*);

- *disaster recovery*;
- *penetration test*.

Per un approfondimento delle procedure rimediali attuate in caso di violazione dei dati personali trattati, si rinvia alla Procedura *Data Breach*.

12. Registro elettronico delle attività di trattamento

Ai sensi dell'art. 30, par. 5 GDPR, il Titolare del trattamento, anche se ha meno di 250 dipendenti, tiene un **Registro delle attività di trattamento**.

Il **Registro dei trattamenti tenuto in qualità di Titolare** contiene tutte le informazioni di cui all'art. 30, par. 1 GDPR e cioè:

- a) il nome e i dati di contatto del Titolare del trattamento e del Responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione internazionale e, per i trasferimenti al di fuori dell'Unione Europea, la documentazione delle garanzie adeguate;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate di cui all'articolo 32, par. 1 GDPR.

Nel caso in cui il **Registro dei trattamenti sia tenuto in qualità di Responsabile**, non occorre indicare le finalità del trattamento, le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, né i termini ultimi previsti per la cancellazione delle diverse categorie di dati; inoltre, le categorie dei dati trattati riguardano i trattamenti effettuati per conto del Titolare (art. 30, par. 2, GDPR).

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante per la protezione dei dati personali, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle dimensioni e della complessità che lo caratterizzano, non può che avere forma elettronica.

13. Nomina del Responsabile del trattamento

KRATOS, ha nominato un unico **Responsabile del trattamento** ai sensi dell'art. 28 GDPR. Il Responsabile è il sig. Marco Ardito, che agisce in qualità di **Responsabile del trattamento e amministratore di sistema**

Il sig. Marco Ardito, in qualità di Responsabile di KRATOS, è stato **autorizzato per iscritto** dalla stessa nel Contratto di nomina del Responsabile del trattamento e amministratore di sistema (*Data Protection Agreement - DPA*), e relativi allegati, sottoscritti tra le parti.

Il rapporto tra KRATOS e il sig. Ardito è espressamente regolato nel *Data Protection Agreement*. In particolare, il Responsabile ha garantito di adottare misure di sicurezza tecniche e organizzative adeguate.

Inoltre, Responsabile ha accesso solo ai dati personali nei limiti di quanto necessario per **l'erogazione dei servizi affidati**.

14. Modello organizzativo *privacy*

KRATOS, in qualità di Titolare del trattamento, oltre al **Responsabile del trattamento**, ha nominato gli **Incaricati del trattamento** ai sensi dell'art. 29 GDPR. Gli stessi sono stati nominati con apposita lettera di nomina sottoscritta da ciascun Incaricato.

Inoltre, per implementare le misure di sicurezza, il Titolare ha nominato un **preposto alla custodia delle parole chiave**, sempre con lettera di nomina - contenete anche le **linee guida** da seguire - la quale è stata sottoscritta dall'Incaricato.

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





Il Titolare del trattamento non ha provveduto, a nominare un **Responsabile per la protezione dei dati (DPO)**, non ricorrendo in uno dei casi di cui all' art 37 GDPR.

Per la completa visione dell'organigramma *privacy* dell'Azienda si rinvia al **modello organizzativo privacy**.

15. Linee guida per gli Incaricati del trattamento

Nel presente Paragrafo e relativi sotto paragrafi ci si soffermerà sulle linee guida degli Incaricati del trattamento, le quali sono state impartite agli stessi prima della nomina.

15.1. Obblighi degli Incaricati

Ciascun Incaricato del trattamento deve:

- rispettare i principi generali del GDPR e della normativa nazionale in vigore, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione dovendole comunicare solo al preposto alla custodia delle parole chiave;
- svolgere le attività previste dai trattamenti secondo le direttive del Titolare del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza esplicita autorizzazione;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il Titolare in caso di incidente di sicurezza che coinvolga dati personali;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237





rispetto delle norme di legge.

15.2. Modalità di svolgimento delle operazioni degli Incaricati

Le principali **operazioni degli Incaricati del trattamento** sono:

- **Identificazione dell'Interessato:** al momento della raccolta dei dati personali, qualora sia necessario individuare l'identità del soggetto che fornisce le informazioni, è obbligatorio richiedere un documento di identità o di riconoscimento, al fine di verificare la identità e di procedere correttamente alla raccolta e alla registrazione delle informazioni.
- **Verifica del controllo dell'esattezza del dato e della corretta digitazione:** al momento della registrazione dei dati raccolti, occorre prestare attenzione alla digitazione e all'inserimento dei dati identificativi e degli altri dati riferiti all'interessato, al fine di evitare errori, che potrebbero generare problemi nella corretta gestione dell'anagrafica e nello svolgimento delle operazioni, che caratterizzano il processo di trattamento.
- **Norme logistiche per l'accesso fisico ai locali:** i locali, ove sono custoditi i dati personali, devono essere soggetti a controllo e a verifica, al fine di evitare che durante l'orario di lavoro possano essere accessibili da parte di soggetti non autorizzati. In caso di allontanamento dai locali aziendali vengono adottate tutte le accortezze e precauzioni al fine di impedire l'accesso fisico a chi non sia legittimato, soprattutto se esterno all'azienda. In particolare, è possibile ricoverare in luogo sicuro i documenti cartacei ed i supporti rimovibili contenenti i dati personali. Pertanto, le porte degli uffici e gli armadi sono dotati di serratura con chiave e, al termine dell'orario lavorativo, vengono sempre chiusi a chiave i locali aziendali nei quali vengono svolti trattamenti di dati personali.
- **Rilevazione presenze:** l'azienda ha una procedura non automatizzata di rilevazione delle presenze e di un servizio di reception/sorveglianza.

15.3. Istruzioni per l'uso degli strumenti informatici

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi.

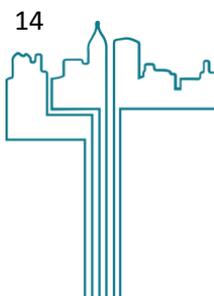
Di seguito sono riportate le **indicazioni per la gestione dei diversi strumenti informatici** per il trattamento dati:

a) Gestione strumenti elettronici (pc fissi e portatili):

Ciascun Incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (es. PC). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione vengono svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro,

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni possono essere comunicate, senza alcuna ulteriore informativa all'interessato.

Per la gestione della sessione di lavoro sul PC, è necessario procedere come segue:

- Al termine delle ore di servizio, i PC devono essere spenti, a meno che non stiano svolgendo elaborazioni particolari. In tal caso gli uffici che contengono tali dispositivi informatici debbono tassativamente essere chiusi a chiave.
- Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto, egli deve chiudere la sessione di lavoro sul PC effettuando il *Logout*, oppure in alternativa deve avere attivo un salvaschermo (*screen-saver*) protetto dalle credenziali di autenticazione. Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
 - non deve mai essere disattivato;
 - il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC;
 - deve essere messo in funzione manualmente ogni volta che si lascia il PC incustodito ed acceso;
- Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.
- Per l'utilizzo dei PC portatili valgono le regole sopra elencate, con le seguenti ulteriori raccomandazioni:
 - prima della riconsegna, rimuovere eventuali file ivi elaborati;
 - quando il PC portatile è nei locali dell'Azienda, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi sicuri dell'arredamento (es. maniglie) utilizzando degli appositi cavi in acciaio dotati di lucchetto;
 - quando il PC portatile è all'esterno dell'Azienda, evitare di lasciarlo incustodito;
 - per assenze prolungate, anche qualora l'ambiente venga ritenuto affidabile, è necessario custodire il PC portatile in modo opportuno (es. cassetto chiuso a chiave o cassaforte);
 - in caso di furto di un PC portatile è necessario avvertire tempestivamente il Titolare e il preposto alla custodia delle parole chiave, onde prevenire possibili intrusioni ai sistemi aziendali;
 - in caso di viaggio aereo trasportare tassativamente il PC portatile come bagaglio a mano;
 - eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

b) Gestione delle credenziali (username e password):

L'accesso al PC fisso o portatile, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un **codice utente (username) ed una parola chiave (password)**. L'adozione ed il corretto utilizzo

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





della combinazione *username-password* è fondamentale per il corretto utilizzo del PC, in quanto:

- tutela l'utente ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue *user id* e *password*) solo lui possa svolgere determinate azioni;
- è necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun incaricato deve scegliere le password la quale, come regola generale, deve essere ragionevolmente complessa e difficile da individuare e/o ricavare. Le credenziali di accesso vengono aggiornate ogni 6 (sei) mesi manualmente, cioè senza scadenze automatiche e digitali impostate. Le credenziali di accesso sono gestite dal preposto alla custodia delle parole chiave secondo quanto previsto nella lettera di nomina contenente anche le relative linee guida.

c) Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su mandato del Titolare del trattamento ovvero direttamente da quest'ultimo. Pertanto, si raccomanda agli Incaricati di rispettare i seguenti divieti:

- Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
- Non installare sistemi per connessione esterne (es: modem wi-fi portatili); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (*shareware*), programmi gratuiti (*freeware*), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
- Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

d) Gestione posta elettronica aziendale

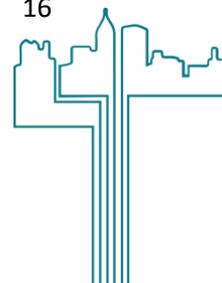
Il servizio di posta elettronica aziendale viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni all'Azienda e in stretta connessione con l'effettiva attività e mansioni dell'Incaricato che utilizza tale funzionalità.

Al fine di non compromettere la sicurezza dell'azienda e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
- È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





- autorizzazione;
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione;
 - Nell'inoltro delle email si raccomanda di prestare attenzione a che:
 - l'indirizzo del destinatario sia stato correttamente digitato;
 - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati appartenenti alle particolari categorie di cui all'art. 9 GDPR;
 - nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

e) Gestione del salvataggio dei dati

Per i dati ed i documenti che risiedono sui *server* gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali *files* distrutti, ad esempio per guasti *hardware* oppure per cancellazioni involontarie.

Per tutti i PC il backup avviene periodicamente (ogni sei mesi). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti, ecc.).

f) Gestione dei supporti rimovibili

I supporti rimovibili, come ad esempio penne USB, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio o cassetto chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati.

Il trasferimento di file contenenti dati personali su supporti rimovibili è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile.

g) Gestione protezione dai virus informatici

Per prevenire eventuali danneggiamenti al *software* causati dalla presenza o dall'azione di programmi virus informatici, su ogni PC dell'Azienda è stato installato un software antivirus aziendale.

L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.

Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al Titolare del trattamento.

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





Si raccomanda di non scaricare e né tantomeno aprire file provenienti via email da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati agli stessi PC.

15.4. Istruzioni per l'uso degli strumenti "non elettronici"

Per **strumenti "non elettronici"** si intendono i **documenti cartacei**.

Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Di seguito sono elencate le istruzioni che gli Incaricati devono seguire:

a) Distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche), ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verificano errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli contenenti dati personali;

b) Misure di sicurezza

Il trattamento sicuro di documenti contenenti dati personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:

- la presenza e l'uso tassativo di armadi e cassette dotati di serratura adeguata;
- la presenza e l'uso tassativo, ove si richieda la distruzione di documenti di un trita carte.

c) Prescrizioni

L'Incaricato deve attenersi alle seguenti prescrizioni:

- in nessun caso è concesso l'accesso a documentazione contenente dati personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- la documentazione contenente dati personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;
- l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i trattamenti previsti;
- i supporti devono essere archiviati in ambiente ad accesso controllato;
- i documenti contenenti dati personali non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

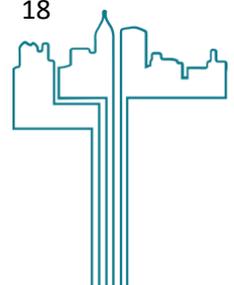
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237

Member of CISQ Federation



CQOP SOA
COSTRUTTORI QUALIFICATI OPERE PUBBLICHE





- il numero di copie di documenti contenenti dati personali deve essere strettamente funzionale alle esigenze di lavoro;
- cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- la distruzione di documenti contenenti dati personali deve essere operata, ove possibile, direttamente dal personale Incaricato;
- ove non siano disponibili strumenti per la distruzione dei documenti (trita carte), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- quando gli atti e i documenti contenenti dati personali sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- l'accesso agli archivi contenenti dati personali deve essere controllato e consentito solo a persone autorizzate;
- è severamente vietato utilizzare documenti contenenti dati personali, come carta da riciclo o da appunti.

16. Linee guida per gli addetti alla manutenzione

Le seguenti istruzioni devono essere osservate dal **personale dei Servizi Informatici ai quali il Titolare si rivolge all'occorrenza**:

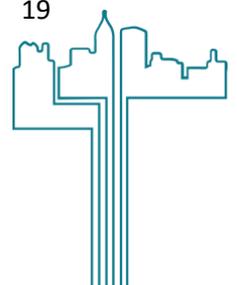
- effettuare operazioni di manutenzione e supporto per verificare il corretto funzionamento (monitoraggio e diagnostica) su flussi dei dati;
- gestire le credenziali di autenticazione dei soggetti incaricati del trattamento su indicazione del Titolare;
- gestire i profili di autorizzazione degli Incaricati al trattamento dei dati, su specifiche impartite dal Titolare;
- provvedere alla disattivazione/variazione delle utenze, ivi compreso l'account di posta elettronica, assegnate al personale cessato dal servizio o che abbia modificato il proprio ambito di trattamento, su richiesta specifica del Titolare
- custodire la documentazione cartacea, prodotta nello svolgimento dei propri compiti istituzionali.

L'accesso agli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico. A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito **eseguire le operazioni strettamente necessarie** a tali scopi e/o richieste dal titolare, secondo le seguenti **istruzioni operative**:

- nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)
P.IVA/C.F.: 13496821003
mail: info@coopkratos.it - pec: kratos.coop@legalmail.it
Tel.: 0683970237





di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare *files* già esistenti ma creare *files* di prova;

- nel caso si renda strettamente necessario accedere a *files* contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione;
- per effettuare operazioni di manutenzione sui *database* aziendali che prevedano la raccolta e la conservazione dei dati, tali dati dovranno essere custoditi in modo tale da non essere accessibili da soggetti non autorizzati.
- devono inoltre essere adottate le misure di sicurezza minime previste dal codice in materia di protezione dei dati personali;
- è necessario informare al più presto il Titolare o il Responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità;
- tutti i dati personali contenuti nei *database* devono essere protetti da password.

Nel caso in cui sia necessario **accedere ai dati attraverso gli strumenti elettronici in dotazione agli Incaricati**, occorre attenersi alle seguenti indicazioni:

- in presenza dell'Incaricato, far digitare la password dall'Incaricato stesso evitando di venire a conoscenza;
- in assenza dell'Incaricato rivolgersi alla persona individuata dall'Incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.

Nei casi in cui sia necessario **accedere ai dati personali attraverso il server**, rivolgersi al Titolare o provvedere, in collaborazione il Titolare alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;

Il Titolare ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;

Qualora si renda **necessario prelevare apparecchiature elettroniche** per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'Incaricato, il quale provvederà a cambiarla al termine delle operazioni di manutenzione.

L'**accesso al sistema informatico** da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;

È assolutamente **vietato comunicare o diffondere i dati personali** di qualsiasi natura provenienti dai *database* gestiti dalla società, se non previa espressa comunicazione scritta.

Nel caso in cui ci si avvalga di **sogetti esterni per interventi specialistici** che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza.

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237



CQOP SOA
COSTRUTTORI QUALIFICATI OPERE PUBBLICHE





17. Sanzioni

È obbligatorio attenersi alle disposizioni in materia di protezione dati personali e di misure minime di sicurezza, ai sensi del GDPR 2016/679 e della normativa nazionale in vigore.

Il **mancato rispetto o la violazione** della normativa applicabile e delle regole contenute nel presente regolamento è perseguibile con **provvedimenti disciplinari nonché con le azioni civili e penali** consentite.

18. Entrata in vigore del regolamento e pubblicità

Il Regolamento *privacy* aziendale entrerà **in vigore il 1° settembre 2018**.

Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti. Copia del regolamento sarà affisso nella bacheca aziendale e verrà reso disponibile mediante comunicazione che ne ufficializza l'adozione nelle forme e con le modalità in uso presso l'Azienda.

19. Aggiornamento e revisione

Il presente regolamento è soggetto a **revisione con frequenza periodica** anche in funzione dell'introduzione di nuovi strumenti di lavoro e/o informatici, dell'evoluzione tecnologica o di cambiamenti normativi.

Allegato 1. Nomina degli Incaricati del trattamento

Allegato 2 Nomina del preposto alla custodia delle parole chiave

Allegato 3 – Line guida e modulo pe l'esercizio dei diritti dell'Interessato

KRATOS Società Cooperativa

Via Leon Battista Alberti, 11 - 00153 Roma (RM)

P.IVA/C.F.: 13496821003

mail: info@coopkratos.it - pec: kratos.coop@legalmail.it

Tel.: 0683970237

