01/07/2026

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI

ai sensi dei D.Lgs. n. 196/2003 e 101/2018 e del GDPR EU 679/2016

Estratto:
Disciplinare per l'utilizzo dei Sistemi Informatici

Sommario

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI..... 0

ai sensi dei D.Lgs. n. 196/2003 e 101/2018 e del GDPR EU 679/2016 **.....0**

1. Dati aziendali ..... Errore. Il segnalibro non è definito.
1.1 Descrizione dell'unità produttiva .....**Errore. Il segnalibro non è definito.**

2. Premessa ..... Errore. Il segnalibro non è definito.

3. Definizioni ..... Errore. Il segnalibro non è definito.

4. Principi di sicurezza e protezione dei dati personali ..... Errore. Il segnalibro non è definito.
4.1 Attuazione .....**Errore. Il segnalibro non è definito.**

5. Elenco dei trattamenti effettuati..... Errore. Il segnalibro non è definito.

6. Analisi dei rischi relativi al trattamento dati ..... Errore. Il segnalibro non è definito.
6.1 Analisi dei luoghi fisici ove si svolge il trattamento di dati personali **Errore. Il segnalibro non è definito.**
6.2 Individuazione e Gestione degli strumenti del trattamento..... **Errore. Il segnalibro non è definito.**

7. Violazione dei dati personali: obbligo di notifica ..... Errore. Il segnalibro non è definito.

8. Disciplinare per l'utilizzo dei Sistemi Informatici 3
8.1 Gestione e protezione delle postazioni ad utilizzo condiviso ('Libero') 4

1. Disciplinare per l’utilizzo dei Sistemi Informatici

Premessa

Ai fini di questo disciplinare si specifica che con il termine “dati” deve intendersi l’insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i “dati personali” intesi a norma di legge.

Inoltre, nell’ambito della sua attività, l’Organizzazione tratta “dati cartacei” ovvero informazioni su supporto cartaceo e “dati digitali” ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell’accezione più ampia sopra descritta, di cui l’incaricato viene a conoscenza, nell’ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l’organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita del titolare del trattamento.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l’attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l’accesso alla rete internet dal computer aziendale espone l’organizzazione a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all’immagine dell’organizzazione stessa. Premesso che i comportamenti che normalmente si adottano nell’ambito di un rapporto di lavoro, tra i quali rientrano l’utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, il Titolare del Trattamento ha adottato il presente Disciplinare Interno diretto a evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Una gestione dei dati cartacei, un uso dei sistemi informatici e dei dispositivi elettronici come computer, notebook, tablet, smartphone, palmari, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc. (di seguito “device”) nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l’organizzazione alla minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell’intero sistema informatico.

Le informazioni contenute nel presente Disciplinare costituiscono parte integrante dell’informativa rilasciata agli Incaricati.

Ai fini del presente disciplinare il Titolare del Trattamento sarà denominato anche come “l’organizzazione”.

8.1 Gestione e protezione delle postazioni ad utilizzo condiviso ('Libero')

- Autenticazione univoca e credenziali personali: È fatto assoluto divieto di utilizzare credenziali di accesso collettive o generiche. Ciascun utilizzatore (inclusi i tirocinanti) deve accedere alla postazione 'Libero' esclusivamente tramite un profilo utente nominativo e password personali forniti dal Titolare.
- Messa in protezione immediata: Vista la natura intrinsecamente condivisa dello strumento, l'operatore o il tirocinante ha l'obbligo tassativo di bloccare lo schermo o effettuare il Logout completo dal sistema operativo e dagli applicativi aziendali prima di allontanarsi dalla postazione, anche per pause di brevissima durata.
- Divieto di memorizzazione locale: È vietato salvare stabilmente sul disco locale della macchina (es. sul Desktop o nella cartella 'Download') file o archivi contenenti dati personali.
- Rimozione dei dati residui a fine sessione: Al termine del proprio turno d'uso o della giornata, l'incaricato o il tirocinante deve assicurarsi di aver chiuso ogni sessione web e di aver svuotato il cestino locale.
- Vigilanza e limitazione dei privilegi per i tirocinanti: In quanto figure in formazione, i tirocinanti operanti sulle postazioni 'Libero' devono disporre di privilegi minimi di accesso ai dati (principio del least privilege), limitati ai soli applicativi e informazioni e seguiti dal tutor aziendale.
- Obbligo di segnalazione: Qualora all'avvio della postazione si rilevino sessioni di altri utenti rimaste aperte, l'utilizzatore deve segnalare immediatamente la situazione al Titolare del trattamento o al tutor aziendale.

1. **Esclusione all’uso degli strumenti informatici**

All’inizio del rapporto lavorativo o di consulenza, l’organizzazione valuta la presenza dei presupposti per l’autorizzazione all’uso dei vari device aziendali, di internet e della posta elettronica da parte degli incaricati.

Successivamente e periodicamente l’organizzazione valuta la permanenza dei presupposti per l’utilizzo dei device aziendali, di internet e della posta elettronica.

E’ fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici dell’organizzazione.

Più specificatamente hanno diritto all’utilizzo degli strumenti e ai relativi accessi solo gli incaricati che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

2. **Titolarità dei device e dei dati**

L’organizzazione è esclusiva titolare e proprietaria dei device messi a disposizione degli Incaricati ai soli fini dell’attività lavorativa.

L’incaricato non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei device aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l’autorizzazione dell’organizzazione.

3. **Finalità nell’utilizzo dei device**

I device assegnati sono uno strumento lavorativo nelle disponibilità dell’Incaricato esclusivamente per un fine di carattere lavorativo. I device, quindi, non devono essere utilizzati per finalità private e diverse da quelle dell’organizzazione, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte di questa Organizzazione, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

4. Restituzione dei device

A seguito di una cessazione del rapporto lavorativo o di consulenza dell’Incaricato con l’organizzazione o, comunque, al venir meno, a insindacabile giudizio dell’organizzazione stessa, della permanenza dei presupposti per l’utilizzo dei device aziendali, gli incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei device in uso.

2. Divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

5. Restituzione dei dati cartacei

A seguito di una cessazione del rapporto lavorativo o di consulenza dell’Incaricato con l’organizzazione o, comunque, al venir meno, a insindacabile giudizio dell’organizzazione stessa, della permanenza dei presupposti per l’utilizzo di dati cartacei aziendali, gli incaricati hanno i seguenti obblighi:

1. Procedere immediatamente alla restituzione dei dati cartacei in loro possesso.

2. Divieto assoluto di alterare o manomettere o distruggere i dati cartacei in loro possesso o renderli inintelligibili tramite qualsiasi processo.

6. Le Password

Le password possono essere un metodo di autenticazione per garantire l’accesso protetto a uno strumento hardware oppure a un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell’organizzazione nel suo complesso. Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è necessario modificarle con una frequenza almeno trimestrale. Inoltre, le password non dovranno essere memorizzate su supporti facilmente intercettabili da altre persone.

Le password che non vengono utilizzate per un periodo superiore ai sei mesi dovranno essere disattivate.

In qualsiasi momento l’organizzazione si riserva il diritto di revocare all’Incaricato il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.

6.1 Regole per la corretta gestione delle password

L’Incaricato, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

- Le password sono assolutamente personali e non vanno mai comunicate ad altri.
- Occorre cambiare immediatamente una password non appena si abbia alcun dubbio che sia diventata poco "sicura".
- Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali (per esempio, i seguenti: { } [ ] , . < > ; : ! ” £ $ % & / ( ) = ? ^ \ | ’ * - + _) e numeri.
- Le password non devono essere memorizzate su supporti facilmente intercettabili, quali ad esempio Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare).
- Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere

dall'esistenza di un sistema automatico di richiesta di aggiornamento password.

- Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell’ente.

- In alcuni casi, sono implementati meccanismi che consentono all'Incaricato fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità contattare il Titolare.

7. Obblighi

L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati aziendale.

L’incaricato deve quindi eseguire le operazioni seguenti:

- Se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti.

- Utilizzare solo ed esclusivamente le aree di memoria della rete dell’ente ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di rete.

- Spegnere il computer, o curarsi di effettuare il Logout, ogni sera prima di lasciare gli uffici o in caso di assenze prolungate, poiché lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l’indebito uso.

- Mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro disposti dall’organizzazione.

- Non dare accesso al proprio computer ad altri utenti, a meno che siano incaricati con cui si condivide l’utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo.

- Bloccare il suo device prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione.

- Chiudere la sessione (Logout) a fine giornata.

- Controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

- Divieti espliciti sull’utilizzo dei sistemi informatici e dei device

All’incaricato è vietato:

- La gestione, la memorizzazione (anche temporanea) o il trattamento di file, documenti e/o informazioni personali dell’incaricato o comunque non afferenti alle attività lavorative nella rete, nel disco fisso o in altre memorie di massa e negli strumenti informatici aziendali in genere.

- Modificare le configurazioni già impostate sul personal computer.

- Utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta dell’organizzazione.

- Installare alcun software di cui l’organizzazione non possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza l’espressa autorizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale.

- Caricare sui device in uso alcun documento, gioco, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate.

- Aggiungere o collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA, ecc.) o periferiche (telecamere, macchine fotografiche, smartphone, chiavi USB ecc.) diversi da quelli consegnati, senza l’autorizzazione espressa dell’organizzazione.

- Creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico dell’organizzazione, quali per esempio virus, trojan horses ecc.

- Accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte.

- Effettuare in proprio attività manutentive

- Permettere attività manutentive da parte dei soggetti non espressamente autorizzati dall’organizzazione.

8. Antivirus

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, ecc.

L’organizzazione impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

L’incaricato, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

- Comunicare al titolare del trattamento ogni anomalia o malfunzionamento del sistema antivirus.

- Comunicare eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all’incaricato:

- È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione.

- E’ vietato ostacolare l'azione dell'antivirus aziendale.

- E’ vietato disattivare l’antivirus senza l’autorizzazione espressa dell’ente anche e soprattutto nel caso sia richiesto per l’installazione di software sul computer.

- E’ vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo sospetti. Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

9. Internet

La connessione alla rete internet dal device avuto in dotazione è ammessa esclusivamente per motivi attinenti allo svolgimento dell’attività lavorativa. L’organizzazione potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni a siti non correlati all’attività lavorativa attraverso filtri e black list.

10. Posta elettronica

L’utilizzo della posta elettronica è connesso allo svolgimento dell’attività lavorativa. In particolare:

- È vietato utilizzare l’indirizzo di posta elettronica contenente il dominio dell’organizzazione per

iscriversi in qualsivoglia sito per motivi non attinenti all’attività lavorativa, senza espressa autorizzazione scritta, nonché utilizzare il dominio per scopi personali.

- È vietato creare, archiviare o spedire, anche solo all’interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, “catene di Sant’Antonio” o in genere a pubblici dibattiti utilizzando l’indirizzo aziendale.

11. Device personali

Ai dipendenti non è permesso svolgere la loro attività su device personali ameno di specifica ed esplicita autorizzazione. In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall’organizzazione e l’eventuale furto o smarrimento del device deve essere immediatamente segnalato per eventuali provvedimenti di sicurezza.

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni) possono utilizzare i propri device personali per memorizzare dati dell’organizzazione solo se espressamente autorizzati e assumendone formalmente e personalmente l’intera responsabilità del trattamento.

12. Utilizzo del cellulare/smartphone personale.

Durante l’orario di lavoro, comprese le eventuali pause, agli Incaricati è concesso l’utilizzo del telefono cellulare personale solo per comunicazioni di emergenza o strettamente collegate all’ambito lavorativo.

Gli Incaricati non dipendenti (ovvero i consulenti e collaboratori esterni) possono utilizzare i propri cellulari/smartphone per memorizzare dati dell’organizzazione solo se espressamente autorizzati e assumendone formalmente e personalmente l’intera responsabilità del trattamento.

13. **Distruzione dei Device**

Ogni device affidato agli incaricati, (computer, notebook, tablet, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.), al termine del suo utilizzo dovrà essere restituito all’organizzazione che provvederà a distruggerlo o a ricondizionarlo seguendo le norme di legge in vigore al momento.

14. **Utilizzo di sistemi cloud**

E’ vietato agli incaricati l’utilizzo di sistemi cloud non espressamente approvati dall’organizzazione. Per essere approvati i sistemi cloud devono rispondere a tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

15. **Clear Desk Policy**

Gli Incaricati sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

Gli Incaricati sono tenuti ad adottare una “politica della scrivania pulita”. Ovvero si richiede agli incaricati di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l’utilizzo degli strumenti digitali messi a disposizione dall’organizzazione.

I principali benefici di una politica della scrivania pulita sono:

- Una buona impressione a clienti e fornitori.
- La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle.
- La riduzione della possibilità che documenti confidenziali possano essere sottratti.

In particolare, si invita a non lasciare in vista sulla propria postazione dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura degli Incaricati riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori, clienti, manutentori, ecc.) presenti in sede.

A fine giornata deve essere previsto il riordino e la corretta archiviazione di tutti i documenti cartacei. Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l’inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.

E’ necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un’apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

16. Il controllo

L’organizzazione, in qualità di Titolare degli strumenti informatici e del trattamento dei dati ivi contenuti, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

- Tutelare la sicurezza e preservare l’integrità degli strumenti informatici e dei dati.
- Evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo.
- Verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico.

17. Modalità di verifica

L’organizzazione promuove ogni opportuna misura, organizzativa e tecnologica, volta a prevenire il rischio di utilizzi impropri e, comunque, a “minimizzare” l’uso di dati riferibili agli Incaricati, e allo scopo ha adottato ogni possibile strumento tecnico, organizzativo e fisico, volto a prevenire trattamenti illeciti sui dati trattati con strumenti

In particolare non vengono adottati sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

Inoltre eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte degli Incaricati avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

Qualora nell’ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all’attività lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà un avvertimento in modo generalizzato con l’invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

18. Modalità di Conservazione

Tutti i dati devono essere conservati per il periodo strettamente necessario. Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in

relazione:

- Ad esigenze tecniche o di sicurezza del tutto particolari.
- All’indispensabilità del dato rispetto all’esercizio o alla difesa di un diritto in sede giudiziaria.
- All’obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell’autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

19. Conseguenze delle infrazioni disciplinari

Le infrazioni disciplinari alle norme del presente Disciplinare Interno potranno essere punite, a seconda della gravità delle mancanze, in conformità alle disposizioni di legge.

20. Modalità di Esercizio dei diritti

Il lavoratore interessato del trattamento dei dati effettuato mediante strumenti informatici ha diritto di accedere alle informazioni che lo riguardano rivolgendosi al Titolare del trattamento.

21. Validità

Il presente Disciplinare valido a partire da: 24/10/2019 è aggiornato alla data del 01/07/2026

22. Aggiornamento

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, o in caso di mutazioni legislative.

Ogni variazione del presente Disciplinare sarà comunicata agli incaricati.

Il Titolare del Trattamento **CONSORZIO “LA RADA”**

Palma Silvestri